IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 24 November 2022, accepted 21 December 2022, date of publication 28 December 2022,
date of current version 2 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3232395

RESEARCH ARTICLE

Evaluation Approach for Efficient Countermeasure Techniques Against Denial-of-Service Attack on MPSoC-Based IoT Using Multi-Criteria Decision-Making

AHMED ABBAS JASIM AL-HCHAIMI[1], NASRI BIN SULAIMAN[1], (Member, IEEE), MOHD AMRALLAH BIN MUSTAFA[1], (Senior Member, IEEE), MOHD NAZIM BIN MOHTAR[1], (Senior Member, IEEE), SITI LAILATUL BINTI MOHD HASSAN[2], AND YOUSIF RAAD MUHSEN[3]

[1]Faculty of Engineering, Universiti Putra Malaysia, Serdang, Selangor 43400, Malaysia
[2]College of Engineering, Universiti Teknologi MARA, Shah Alam, Selangor 40450, Malaysia
[3]College of Engineering, University of Wasit, Kut 52001, Iraq

Corresponding author: Ahmed Abbas Jasim Al-Hchaimi (al-hchaimi.ahmed@student.upm.edu.my)

ABSTRACT ***Context:*** Denial-of-Service Attack countermeasure techniques (DoS A-CTs) evaluation is a Multi-criteria decision-making (MCDM) problem based on different MPSoCs of IoT platform design, performance, and design overhead. Therefore, the Fermatean by fuzzy decision opinion score method (F-FDOSM) for prioritizing the powerful countermeasure technique against Denial-of-Service (DoS) attack is the best approach because it employs the most efficient MCDM ranking technique. Nonetheless, the FDOSM method needs to weight the criteria before being submitted for the ranking process. In order to address this theoretical challenge, the Criteria-importance through inter-criteria correlation (CRITIC) technique can be applied as an effective MCDM weighting technique to offer an explicit weight for a set of criteria with no inconsistency based on the standard deviation, which uses correlation analysis to determine the relevance of each criterion. ***Objectives:*** This research proposes a Fermatean-FDOSM framework for evaluating DoS A-CTs in the context of MPSoCs-based IoT and CRITIC techniques to weight the criteria. ***Methods:*** The methodology is presented in three phases. Firstly, a proposed countermeasure techniques dataset was collected that included eighteen defense approaches (e.g., Sniffer, SeRA, and RLAN) based on thirteen criteria (e.g., size, power, latency, and effectiveness …etc.). Then, the Decision matrix (DM) was built based on an intersection of the countermeasure techniques as an alternative and MPSoC design and performance criteria. Then, the multi-criteria decision-making methods were integrated. The CRITIC method for criteria weighting was followed by the development of the Fermatean-FDOSM method for ranking. ***Results:*** (1) CRITIC weighting shows that MPSoC NoC Routing Algorithm (XY and YX) is the highest weight criterion, whereas latency (clock/cycle) is the less weight criterion. (2) The Fermatean-FDOSM-based group ranking shows that the Collision Point Router Detection (CPRD) countermeasure technique is the first-ranked alternative compared to the Secure Model Checkers (SMCs) approach. (3) The DoS A-CTs priority ranks were subjected to a systematic ranking that was confirmed by solid correlation results throughout thirteen criterion weight values. A comparison with recent studies confirmed the feasibility of the proposed framework. ***Conclusion:*** The results of this research are expected to provide a specific understanding and guide for those who want to engage in MPSoCs-based IoT and NoC communication security research with decision theory.

The associate editor coordinating the review of this manuscript and approving it for publication was Alba Amato.

INDEX TERMS Network-on-chip security, multiprocessor system-on-chip, denial-of-service attack, countermeasure techniques, multi-criteria decision making, CRITIC, fermatean fuzzy set FDOSM.

I. INTRODUCTION

A. MOTIVATION

The tremendous advancement in computational systems has resulted in the adoption of parallel architectures using Multiprocessors System-On-Chip (MPSoCs). Mainly, the IoT is based on MPSoCs devices that have become more complicated and powerful and thus are linked together through a 5G network [1], [2]. However, due to their extensive use in critical applications and resource sharing, MPSoCs have become prone to hardware and software attacks that might denial the service, physically damage the system, compromise crucial information, or interrupt the running application [3]. Attacks on MPSoCs may perform on either a computational level, i.e., Intellectual property (IP) cores such as processors, memory blocks, I/O peripherals, and so on, or a communication level, i.e., Network-On-Chip (NoC) [4]. This fact also offers an extreme threat to semiconductor suppliers and ultimate MPSoCs customers, including vital applications and cyber infrastructure; given the current circumstances, including military weaponry, mobile communications, aerospace agencies, and medical electronics, it is not only necessary but also challenging to research several defensive approaches and Countermeasure techniques (CTs) in order to mitigate the possible risks to data security presented via what is known as DoS attacks, explicitly Flooding and Distributing Flooding-DoS.

B. CHALLENGES

Because of the growing attention shown by academia and industry, research on DoS A-CTs in the context of MPSoCs-based IoT remains scarce in the literature. The majority of published research articles have concentrated on the MPSoC communication security aspects and several expected Hardware Trojans (HTs) and other malicious circuits that may include in the MPSoC platforms by a disloyal member during the design or fabrication process [5]. Some studies have focused on the MPSoCs communication system routing protocols and routers aspects, highlighting the necessity of the proposed defenses techniques compatible with MPSoC design constraints or investigating the appropriate countermeasure technique for MPSoC in real runtime [6], [7], [8], [9]. We provide a methodology that helps facilitate both design and implementation aspects of selecting powerful countermeasure techniques against DoS attacks in the context of MPSoCs-based IoT.

In general, choosing the suitable criteria to assess the countermeasure technique against DoS A-CTs in the context of MPSoCs-based IoT leads to performance enhancement and robust MPSoC platforms. From this perspective, MCDM methods are beneficial for devising a system for picking the optimal countermeasure technique against DoS attacks in the context of MPSoCs-based IoT. In an MCDM method, many criteria are evaluated, and a total score is given to each alternative depending on the assessment, which is often offered by a group of experts (decision-makers). Moreover, experts must inevitably deal with inadequate and imperfect evidence due to the subjective nature of their decisions. In this way, fuzzy set theory [14] offers valuable tools to aid experts in making the right decision by giving more robust and precise results.

C. CONTRIBUTION

The current study aims to present an integrated CRITIC method with Fermatean-FDOSM for decision-making under uncertainty for weighting and ranking countermeasure techniques of DoS attacks in the context of MPSoCs-based IoT. Briefly, this article's key contributions are as follows:

1) This study fills the gap in evaluating the different approaches of defense against DoS attacks in the context of MPSoCs-based IoT.
2) The detailed analysis proposes a decision matrix for DoS A-CTs includes thirteen criteria and eighteen alternatives.
3) For the first time, this study integrated CRITIC with Fermatean-FDOSM.
4) For the first time, this study employs the CRITIC method to wight DoS A-CTs criteria.
5) For the first time, this study utilizes the Fermatean-FDOSM method with MPSoCs-based IoT countermeasure techniques decision matrix to find the most efficient countermeasure technique.

In addition, this study uses the individual and group approach of ranking to select the most potent countermeasure technique against DoS in the context of MPSoCs.

D. OBJECTIVES

In this article, we intend to achieve the following goals:

1) Providing an efficient and systematic technique to the problem of selecting powerful countermeasure techniques against DoS attacks in the context of MPSoCs-based IoT.
2) Offering an accurate formal representation for experts' often vague or unclear subjective assessments.
3) Giving a solid example (case study) demonstrating the relevance and effectiveness of the suggested countermeasure techniques against DoS attacks in the context of MPSoCs-based IoT with ambiguous and unclear information.
4) Presenting insights to practitioners and academics about decision support systems in the embedded system security domain.

E. SIGNIFICANCE AND IMPLICATIONS

1) MPSOC ROLE IN IOT

Internet-of-Things (IoT) environment was recently built upon MPSoCs platforms ultimately [10]. The MPSoCs have become a legitimate platform for computing and may be used in various computationally intensive real-time applications. MPSoCs in IoT can be employed in a vital aspect such as healthcare and automated assistance (e.g., STMicroelectronics MPSoC), multimedia surveillance (e.g., Xetal-I (128 processors) and Xetal-II (320 processors), environment monitoring, and industrial applications (e.g., Xilinx Zynq® UltraScale™). Incorporating MPSoCs into the IoT paradigm creates new potential and security challenges. When building MPSoCs, keeping strict real-time limitations and security needs in mind is essential. When these seemingly incompatible requirements must be met, NoC solutions become crucial. For example, the NoC architecture significantly impacts the system's security. A vital security threat called a Denial-of-Service (DoS) attack based on NoC communication system degradation, battery lifespan loss, quality of service violations, and quality of service breakdown. Firstly, FIGURE 1 illustrates MPSoCs with a varied array of Processing elements (PEs) as Intellectual property (IP) cores that provide parallelism and programmability, resulting in power efficiency, powerful processing performance, and more flexibility, leading to reduced communication latencies in huge environments such as IoT cloud edges. Secondly, the typical DoS attack scenario is based on system degradation. The adversary looks to degrade the system performance of either computation or communication.

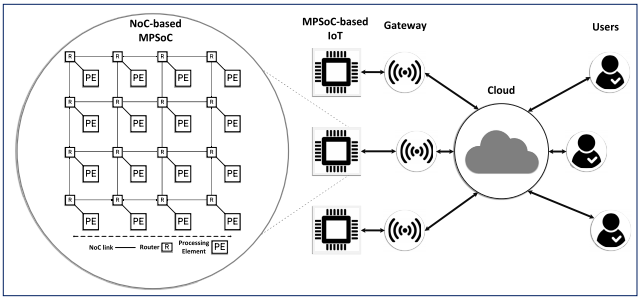

FIGURE 1. MPSoC-based IoT, adopted from [11].

In a domain like that depicted in FIGURE 1, end users submit their scripts or an application for implementation by MPSoC-powered IoT platforms. Following that, the task scheduler of IoT platform firmware maps an application to the IP cores of the integrated MPSoC on a typical operation. Unfortunately, the client might submit one or more of these applications to launch a DoS attack on the MPSoC Network-On-Chip (NoC).

Furthermore, NoC flooding is the primary frequent DoS attack approach. A malicious program executing on any infected IP core of MPSoC can perform by sending packets to another IP core over the NoC. These extra packets compete for the routers' crossbars in the same communication path and, if successful, prevent the transmission of other packets. The blocked packet has forwarding delays increased, resulting in an overall extra communication delay that time considered unacceptable from the perspective of crucial applications.

2) NOC ROLE IN MPSOC

NoC is the heart of MPSoC. NoC is an expanding technology for the formation of multiprocessor state interconnect patterns. NoC technology is modified to accommodate various multiprocessor needs. NoC gives MPSoC components a way to talk to each other that is reliable, fast, scalable, and uses little power [2], [12], [13], [14]. NoC is an interconnection design that consists of many processing elements linked to one another by routers and regular-sized wires (links). As seen in FIGURE 2, a processing element may be anything from a microprocessor to an Application-specific integrated circuit (ASIC) to a chunk of Intellectual properties (IPs) cores that execute a particular program. However, PEs are referred to as IPs throughout this study.

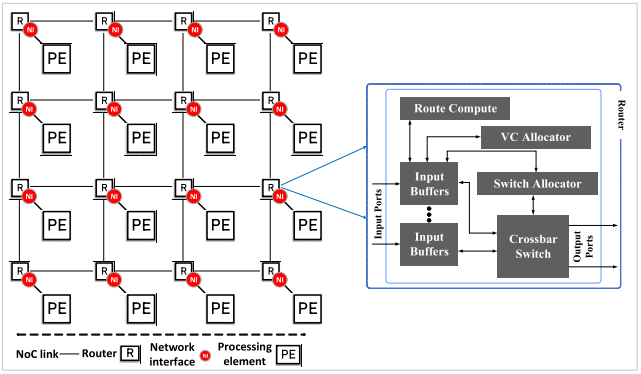

FIGURE 2. 4 × 4 NoC-based MPSoC with basic NoC router architecture.

FIGURE 2 illustrates the typical NoC building blocks. The first NoC main component is an NoC router, a crossbar-based hardware component that switches incoming packets to the output ports of the targeted IP core. NoC router control NoC transmission medium known as links. NoC router connects MPSoC IP cores in a pre-defined methodology called a topology. The source IP injects the packets of data to be received by the destination IP. Typically, NoC routers integrate several components, such as input buffers and a crossbar switch, in addition to the allocator that assigns the priority and schedulable to packets for granting crossbar access. The second NoC component is the Network interface (NI). NI is used to link IP cores to routers. NI executes the communication protocol for managing packing and unpacking data in addition to data injection and ejection from the NoC [15]. NoC connectivity architecture employs a packet-based communication strategy. A request or response (source/destination) model directed to a cache or off-chip memory is separated into packets, which are then converted to flits and injected into the network. A flit is the smallest flow control unit in

an NoC. Packets may be made up of one or more flits routed by NoC routers.

3) WHY CHOOSING CRITIC

Diakoulaki suggested the Criteria-importance through inter-criteria correlation (CRITIC) as a robust criteria weighting approach [16]. CRITIC is an objective technique for estimating the weight of criteria in a decision-making challenge that includes a degree of conflict and contrast. CRITIC is a correlation approach that uses an analytical computation of a decision matrix to determine the information contained in the criteria used to evaluate alternatives. The CRITIC technique comprises of six steps, and the standard deviation of normalized criterion values by columns, as well as the correlation coefficients of all pairs of columns, are utilized to calculate the criteria contrast [16], [17], [18], [19]. The CRITIC technique stages for extracting the DoS A-CTs DM criterion wights are explained in Section III, of this study.

4) WHY CHOOSING FDOSM

The Fuzzy decision by opinion score method (FDOSM) is one of the recent MCDM approaches introduced in the current studies by Salih [20]. FDOSM proposes a stable and efficient MCDM approach under a fuzzy environment. The FDOSM method has been proposed in order to yield the fewest mathematical operations, define a fair and implicit understandable comparison, stop inconsistency, and cut down on vagueness [20], [21], [22]. The FDOSM method is based on three phases, called (data input, transformation, and processing phase) respectively. FDOSM utilizes individual and group decision-making platforms. FDOSM procedure basis on the principle of ideal solutions and enables the experts (decision makers) to identify and select the best value and compare it with other values based on the same criterion. Consequently, a different mathematical operation should be performed to get the final rank and select the best alternative among a set of available alternatives. FDOSM has already been proven to be quite powerful when combined with fuzzy approaches and conflicting criteria [22], [23], [24], [25], [26], [27], [28].

In this study, we apply the FDOSM MCDM method with Fermatean Fuzzy Set (FFS) within the context of alternative ranking to select the most potent DoS countermeasure technique.

5) WHY WORKING WITH FERMATEAN FUZZY SETS

In Yager developed the theory of Fermatean fuzzy sets (FFSs) [29]. FFSs are a novel extension of Pythagorean fuzzy sets (PyFSs) [30] and Intuitionistic fuzzy sets [31]. Since the total of the cubes of the membership and non-membership degrees of FFSs is in the unit interval, FFSs give a broader viewpoint on fuzzy sets. They allow experts more flexible to express their opinions about membership ratings [32], [33], [34]. In order to manage uncertain information, FFSs are more adaptable and effective than IFSs and PyFSs. As a result, using FFSs to represent decision-making uncertainties when adapting DoS A-CTs DM offers an advanced assessment of the significance of main and sub-criteria, an accurate evaluation of experts' reputations, and an effective assessment of explored alternatives as we used in the current study. FFS-based models have previously been used to resolve MCDM issues in the fields of Cyber Security Technologies, IoT, and Quantum Communication Evaluation [35], [36], [37], [38]. However, there has not been any prior study that offers an FFS-based MCDM model for DoS A-CTs in terms of MPSoCs of IoT.

II. LITERATURE REVIEW

The review of literature is divided into three sections. First, we discuss a number of the current research lines and studies on the MPSoC of IoT DoS attacks, threat models, and DoS countermeasure techniques. The second section focuses on CRITIC and FDOSM methods. The last section focuses on recent Fermatean Fuzzy Sets (FFSs) research.

A. STUDIES ON DOS ATTACKS OF MPSOCS-BASED IOT

Due to the global utilization of embedded systems, MPSoC is commonly used in embedded systems. An efficient and scalable connectivity architecture, NoC allows several cores to communicate with one another inside the MPSoC. In the MPSoC, several tasks run simultaneously on different processors that all connect to the same NoC. As a result, the NoC is now a prime target for threats and security attacks. One of the crucial attacks affecting the MPSoCs platform's performance and buying intention of today's semiconductor industries is a malicious circuit known as a Hardware Trojan (HT), which might infect the NoC and launch a DoS attack. Among the most recent research, Daoud offers a DoS attack model for Hardware HT that works by purposefully deleting packets from the NoC. Dropping packets due to infection earns the infected router another name: Black hole router [1]. Daoud also provides a countermeasure technique as a secure connectivity network. The suggested method can identify and localize the BHR in real-time, then cut it off from the network routing by rerouting the packets around the compromised router [39]. Chaves et al. analyze information to narrow down the attacker's position in the MPSoC, reducing search space by 69%; then, they propose a low-cost approach for detecting interference by upgrading communication packet structure and putting communication degradation monitors in NoC routers [40]. Khalid et al. introduce a general technique to identify runtime intrusions using burst mode communication. Their three-phased approach is behavioral modeling of design specifications and linear temporal logic model checker verification. Secondly, Phase 1 counterexamples are used to introduce runtime monitors. Finally, install and test runtime monitoring. The suggested approach may be utilized to create a runtime monitoring configuration without IP module netlist information [41].

Understanding matching Machine learning (ML) algorithms and approaches as a powerful technique for hardware security attacks detection and localization of malicious

IP cores constitute the trend research direction currently followed by DoS attacks and countermeasure techniques in several studies. Sinha et al. present a Sniffer, an effective MIP localization system that leverages a low-overhead machine learning technique to precisely track the attack route and make a consensus conclusion about the location of the MIPs [3]. Charles et al. [42] suggest a system that is both efficient and light on resources, allowing it to identify them as they occur in real-time time. When an attack is detected, their method may additionally pinpoint the location of the offending IP core by analyzing the latency data collected by NoC devices. In addition, Charles et al. developed the proposed system in [42] to be an effective system for detecting and localization Distributed DoS (DDoS) attacks in real-time. They provide a real-time, lightweight approach for detecting DDoS attacks on NoC-based SoCs by analyzing packets for infractions. Using the latency data from the NoC routers after a possible attack has been identified, our method can additionally localize the malicious IPs. During the design phase, apps are statically profiled to discover communication patterns. These patterns are then used for real-time DDoS detection and localizations [43].

B. DOS ATTACKTHREAT MODEL

This section categorizes the DoS attacks in the context of MPSoC-based IoT according to the threat motel. The threat model is a methodology based on pre-identified steps implemented by a system attacker [40]. In general, DoS attacks almost shares the same characteristics regarding threat models in the context of MPSoCs-based IoT except for a few improvements by attackers or system designers in terms of improving their DoS attacks countermeasure techniques against proposed DoS strategies (e.g., DoS and DDoS) attacks. In real runtime, MPSoCs running in the context of IoT can download programs that update the firmware and perform several dynamic applications. Due to executing such operations, system adversaries plan to infect a pre-defined IP core to produce a Malicious IP (MIP) capable of flooding the system with useless packets to degrade the system's performance. Then enables system adversaries to exploit system degradation to accomplish various tasks, such as extracting sensitive data or depriving the system's service. FIGURE 3 depicts the typical DoS attack steps on MPSoCs-based IoT. There are steps to perform the framework of DoS attacks starting by infecting an IP core with malicious software (e.g., Malware or Hardware Trojan) to control the SoC communication infrastructure. The MIP initializes the Packet injection rate (PIR) to neighbor IPs to maintain the connection and calculate the effectiveness of PIR on the system. MIP keeps flooding the system by maintaining the same high rates of PIR until the DoS conditions are satisfied.

There are three DoS attack threat models (1) Packet corruption DoS (2) Flooding DoS (3) Traffic Manipulation DoS, depending on their threat model.

1) PACKET CORRUPTION DOS

It is a DoS attack that may also be caused by continuous packet corruption [44]. For example [45], hardware Trojans interfere with flits arriving at a router's input buffer, causing performance reduction. Dropped packets, waste of NoC resources such as buffer space, response delays, and retransmissions contribute to performance loss. This proposed category of DoS attacks is a result of four different sorts of (a) Hardware trojans, (b) Head Hardware trojans, (c) Tail HT Addresses, and (d) Quan HT.

2) FLOODING DOS

It is a DoS attack that relies on malicious IPs that may cause DoS attacks by flooding the NoC with packets in an attempt to manipulate the availability of on-chip resources. A SoC's performance may rely substantially on only a few parts. An application that makes significant use of memory, for instance, will cause increased traffic on the routers linked to the memory controllers [42], [43] as shown in FIGURE 3.

3) TRAFFIC FLOW MANIPULATION DOS

It is a DoS attack that depends on unfair packet treatment at the NoC router [46]. Once incorporated into the SoC, the Malicious NoC IP (MIP) manipulates traffic to/from a critical Victim IP (VIP). Denying router allocator and arbiter equitable access controls traffic flow. The allocator gives flits crossbar access. Allocator delays packets to/from victim IP to cause DoS. At the arbiter, the Trojan-infected router assigns victim IP flits the least priority.

C. DOS ATTACK COUNTERMEASURE TECHNIQUES

This section classifies DoS attack countermeasure techniques for NoC-based MPSoCs according to the DoS attack threat model as in below:

1) ADDITIONAL CHECK VALIDATION

DoS countermeasure technique based on functional validation; validation methods are often used. For example, Secure Model Checkers, NoC Alert, and NoC Router characteristics to avoid DoS attack on MPSoCs-of IoT are a defence approach proposed in [47], [48], [49], [50], and [51].

2) TRAFFIC FLOW MONITORING

DoS countermeasure technique based on abnormalities of traffic flow monitoring procedure. For example, in articles [42], [43], [52], [53], [54], the DoS attacks proposed are based on injecting additional packets into the network and then examining their latencies. And the countermeasure techniques rely on profiling SoC behaviour in order to detect DoS attacks. The profile is statically identified the time window and the maximum number of packets that should arrive at the NoC router; if it exceeds these limits, it will be flagged as a potential threat.

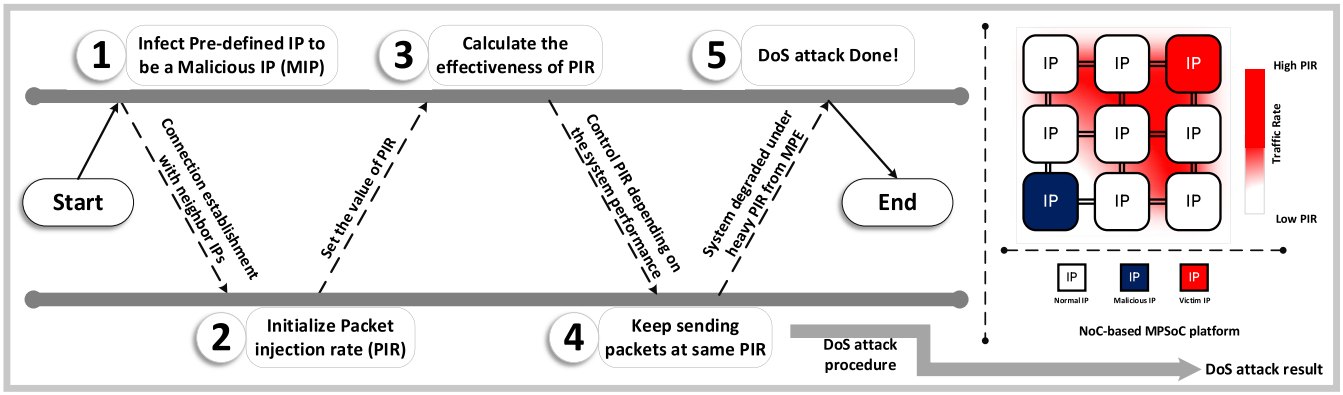

FIGURE 3. DoS attack essential steps.

3) FUZZING AND PARTITIONING

The DoS countermeasure technique is based on making HT task more complicated and difficult. For example, in articles [44], [45], [48], designers proposed a defense approach based on bit-shuffling and SurfNoC architecture methods to mitigate the attack effectiveness. Bit-shuffling makes packets less vulnerable to attack by reordering the packets' crucial bit fields so that the Trojan targets random data rather than the packets' required fields. Frequently, the order of the shuffles will alter. Since the Trojan does not know the reshuffling patterns, it cannot meaningfully target specific fields in an attack. At the same time, the SurfNoC technique enhances security and performance issues by dividing the information carried by the NoC into (domains) and transmitting (waves) of information from each part via the NoC in turn. The concept of waves may be thought of as a temporal division. Because of this, only packets of the same kind may ride the wave without affecting other channels. Consequently, packet latencies are decreased, and attacks aimed at depleting bandwidth or launching denial-of-service attacks are mitigated.

D. STUDIES ON CRITIC

There are several uses of the CRITIC approach in recent studies. Bertozzi and Benini [13] used the combinative distance-based assessment method coupled with CRITIC to investigate the end-milling operation of AISI 1522H steel grade under minimum-quantity lubrication conditions. Wolf et al. [14] employed the CRITIC technique to provide a trust evaluation method for service composition in cloud manufacturing. Ali et al. [10] presented a stakeholder assessment based on the qualities that stakeholders possessed, mainly relying on the evaluation of attribute weights utilizing the CRITIC technique to resolve any potential link between the attributes in estimating their weight. Zhou et al. [15] analyzed the effectiveness of delta-shaped barriers in a solar water heating system using CRITIC. The complex proportional assessment technique was used to identify the best design option. Diakoulaki et al. [16] established a thorough evaluation strategy to assess and rank the energy sources using statistical data and the CRITIC technique to weigh qualities. In Gaur et al. [17] used CRITIC to determine the relative importance of the multidimensional values to estimate the architectural heritage value for its management. In addition, Silvius and Schipper [18] utilized the hybrid criteria significance through CRITIC and multiplicative exponent weighting optimization techniques to choose the best brake friction formulation that achieves the highest performance standards. Stević et al. [19] suggested a solution to address the double normalization-based multiple aggregation approach of linguistic D numbers using the CRITIC technique.

In our study, it is a significant contribution given that, to the best of our knowledge, this is the first time the CRITIC approach was utilized for weighting DoS A-CTs DM criteria.

E. STUDIES ON FDOSM

The FDOSM is a novel MCDM method for ranking the alternatives [20]. FDOSM was proposed recently by Salih, and several notable articles have been dedicated and implemented as a valid alternative to MCDM techniques, resulting in practical applications in different research areas. FDOSM has already been applied to evaluate the sign language system of recognition-based data glove wearable electronic devices in using an Interval-Valued Pythagorean Fuzzy Set with FDOSM as IVP-FDOSM with an assistance of a panel of three experts [23]. In particular, an increasing number of articles deal with applications of FDOSM for efficient (COVID-19) vaccine distribution and related aspects. Among others, [21], [27], [28] utilize FDOSM with FWZIC + q-Rung Orthopair Fuzzy and Pythagorean Fuzzy, respectively, to either prioritize the vaccine recipients or assess the vaccine doses distribution also with the help of three experts panel. In addition, Mahmoud et al. proposed a model using the Intuitionistic FDOSM method to evaluate the data equation system types for supporting the designers and industries of auto-drive vehicles with the help of three experts [25]. Moreover, Mahmood et al. proposed a benchmarking framework for evaluating network congestion control methods of active queue management approach using FDOSM with

interval type-2 trapezoidal fuzzy decision with the support of six experts. Furthermore, Alamoodi et al. developed a benchmarking model for innovative electronic-tourism applications using FDOSM with fuzzy weighted with zero inconsistency method and supported the opinion of eleven expert panels [24].

F. STUDIES ON FFSs

Zadeh laid the basis of the Fuzzy Set (FS) theory in [55]. FS is presented to employ language concepts and degrees of membership in decision-making methods to deal with the ambiguity and imprecision that are a part of human judgment. A class of items with gradations of membership is known as an FS. These rankings show a particular element's stability inside an FS [56]. However, increasing MCDM approaches and methods have introduced what are called Fermatean Fuzzy Sets (FFSs) [57] that can manage uncertain information more readily throughout the decision-making to assess the DoS A-CTs in the current study. TABLE 1 lists more recent contributions in terms of FFSs.

TABLE 1. Typical recent studies in terms of FFSs.

Article - Year	Contribution
[58]-2019	Developed a Fermatean fuzzy WPM decision algorithm to choose the best type of bridge to build.
[59]-2020	In order to expand the flexibility of information aggregation, TOPSIS was extended to Fermatean fuzzy sets based on numerous novel Dombi operators.
[60]-2021	The ideal location for a medical waste disposal facility was determined using a group decision model developed using entropy, a scoring function, and f weighted aggregated sum product assessment method.
[61]-2022	By combining the Fermatean Fuzzy method with the extensions of SAW, ARAS, and VIKOR, a suitable COVID-19 testing facility was identified.
[62]-2021	Established a sustainable third-party reverse logistics provider evaluation technique by integrating CRITIC and EDAS with a unique generalized scoring function of the Fermatean Fuzzy Set.
[63]-2021	Proposed the CRITIC-COPRAS Fermatean fuzzy approach to deal with the problems of long-term digital transformation.
[64], [65]-2021	Produced the TODIM and TOPSIS algorithms with the suitable Fermatean fuzzy linguistic set utilizing novel distance measures based on linguistic scale functions.
[66], [67] - 2022	Proposed a model to prioritise the COVID-19 patients for Mesenchymal stem cell transfusion and COVID-19 Machine Learning methods using Fermatean-FDOSM with fuzzy weighted with zero inconsistency for criteria weighting and ranking.

FFSs have five general definitions [29], as in below:

1) DEFINITION 1

The non-empty set (X) is defined as the intuitionistic fuzzy sets with objects in the form of:

$$A = \{\langle \mathrm{x}, \alpha_{\mathrm{A}}(\mathrm{x}), \beta_{\mathrm{A}}(\mathrm{x})\rangle : \mathrm{x} \in \mathrm{X}\} \tag{1}$$

where $\alpha_A(x) : X \to [0, 1]$ and $\beta_A(x) : X \to [0, 1]$, depicts the degree of membership and non-membership of each element $x \in X$ to the set (A) individually, as well as $(0 \leq \alpha_A(x) + \beta_A(x) \leq 1)$ for all $(x \in X)$. Explicitly, the set (A) becomes a fuzzy set when $\beta_A(x) = 1-\alpha_A(x)$ for every $(x \in X)$.

2) DEFINITION 2

Let $\bar{\mathrm{A}} = (\alpha_{\mathrm{A}}, \beta_{\mathrm{A}})$ and $\bar{\beta} = (\alpha_{\mathrm{B}}, \beta_{\mathrm{B}})$ Two FFS and $(\partial > 0)$, then their operations are defined as follows:

$$\bar{\mathrm{A}} \boxplus \bar{\beta} = \mathrm{w}_* \left(\sqrt[3]{\alpha_{\mathrm{A}}^3 + \alpha_{\mathrm{B}}^3 - \alpha_{\mathrm{A}}^3 \alpha_{\mathrm{B}}^3}, \beta_{\mathrm{A}} \beta_{\mathrm{B}} \right) \tag{2}$$

$$\bar{\mathrm{A}} \otimes \bar{\beta} = \mathrm{w}_* \left(\alpha_{\mathrm{A}} \alpha_{\mathrm{B}}, \sqrt[3]{\beta_{\mathrm{F}_1}^3 + \beta_{\mathrm{F}_2}^3 - \beta_{\mathrm{F}_1}^3 \beta_{\mathrm{F}_2}^3} \right) \tag{3}$$

$$\partial.\bar{\mathrm{A}} = \mathrm{w}_* \left(\sqrt[3]{1 - \left(1 - \alpha_{\mathrm{F}}^3\right)^{\partial}}, \beta_{\mathrm{F}}^{\partial} \right) \tag{4}$$

$$\bar{A}^{\partial} = \mathrm{w}_* \left(\alpha_{\mathrm{F}}^{\partial}, \sqrt[3]{1 - \left(1 - \beta_{\mathrm{A}}^3\right)^{\partial}} \right) \tag{5}$$

where (w) is a criterion weight resulted by applying CRITIC weighting method, see PHASE 2: CRITERIA WEIGHTING.

3) DEFINITION 3

Let $\bar{A} = (\alpha_A, \beta_A)$ is FF, (S) is the score, and (T) is the accuracy function respectively, then:

$$\mathrm{S}(\bar{\mathrm{A}}) = \alpha_{\mathrm{A}}^3 + \beta_{\mathrm{B}}^3 \tag{6}$$

$$\mathrm{T}(\bar{\mathrm{A}}) = \alpha_{\mathrm{A}}^3 + \beta_{\mathrm{B}}^3 \tag{7}$$

The above Equation (6) and Equation (7) can be used to compare two FFs, $\bar{A} = (\alpha_A, \beta_A)$ and $\bar{\beta} = (\alpha_B, \beta_B)$. In order to compare these two FFs there are three different conditions as listed below:

1) If $\mathrm{S}(\tilde{\mathrm{A}}) < \mathrm{S}(\tilde{\bar{\beta}})$, then $\tilde{\mathrm{A}} < \tilde{\bar{\beta}}$
2) If $\mathrm{S}(\tilde{\mathrm{A}}) > \mathrm{S}(\tilde{\bar{\beta}})$, then $\tilde{\mathrm{A}} > \tilde{\bar{\beta}}$;
3) If $\mathrm{S}(\tilde{\mathrm{A}}) = \mathrm{S}(\tilde{\bar{\beta}})$, then:
   - $\mathrm{T}(\tilde{\mathrm{A}}) < \mathrm{T}(\tilde{\bar{\beta}})$, then $\tilde{\mathrm{A}} < \tilde{\bar{\beta}}$
   - $\mathrm{T}(\tilde{\mathrm{A}}) > \mathrm{T}(\tilde{\bar{\beta}})$, then $\tilde{\mathrm{A}} > \tilde{\bar{\beta}}$;
   - $\mathrm{T}(\tilde{\mathrm{A}}) = \mathrm{T}(\tilde{\bar{\beta}})$, then $\tilde{\mathrm{A}} = \tilde{\bar{\beta}}$.

4) DEFINITION 4

Let FFs $\bar{A} = (\alpha_A + \beta_A)$ expresses the FFs complement; then the complement can be defined as:

$$\mathrm{Com}(\tilde{\mathrm{A}}) = (\beta_{\mathrm{A}}, \alpha_{\mathrm{A}}) \tag{8}$$

5) DEFINITION 5

As mentioned in definition 3, the score Equation (7) of FFs has defined assuming FFs is $\bar{\mathrm{A}} = (\alpha_{\mathrm{A}}, \beta_{\mathrm{A}})$ where the value of $(\mathrm{S}^{\ddot{A}})$ should be withing the range of (-1 to 1). Equation (9) shows the positive score function

$$\mathrm{S}^{\mathrm{p}}\left(\tilde{\mathrm{A}}_{\mathrm{ij}}\right) = 1 + \mathrm{S}\left(\tilde{\mathrm{A}}_{\mathrm{ij}}\right) \tag{9}$$

III. METHODOLOGY

This section contains a comprehensive overview of the suggested methodology. This methodology aims to achieve

an MPSoCs-based IoT DoS A-CTs evaluation framework depending on the utilized CRITIC and Fermatean-FDOSM methods. The first phase of this methodology is detailed in Section A, which describes the DoS A-CTs DM construction and definition process. Afterward, Section B shows the CRITIC objective weighting method of the DoS A-CTs DM phase. Finally, Section C presents the ranking process by using the Fermatean-FDOSM method to the alternatives of DM mentioned in Phase 1 and using criteria weights resulting in Phase 2. The evaluation framework of DoS A-CTs using CRITIC and Fermatean-FDOSM is illustrated in FIGURE 4. Methodology phases.

A. PHASE 1: DM BUILD AND DEFINITION

In this phase, the DM in was used to evaluate DoS attack Countermeasure techniques based on their Design Metrics, Performance Metrics, Design Overhead, and Security Metrics as criteria and defenses methods as an alternative were discussed. The standard selection of mentioned aspects was conducted according to a comprehensive investigation of the prior studies mentioned in Section II. Authors in the previous studies pay more attention to the design metrics of MPSoC when they propose a new defense approach against DoS attacks in MPSoC. Also, they check the platform performance metrics by applying different applications, task mapping, and comparing the results before/after implementing the defense approach. In addition, there are high constraints on the additional costs resulting from applying such countermeasure techniques, which refers to design overhead. Furthermore, the methodology and threat models followed by an adversary to compromise NoC-based MPSoC platforms to implement the DoS attack are the security metrics of platform vulnerabilities in order to implement the DoS attack. Consequently, the mentioned aspects are considered vital and should be available in any countermeasure technique against a DoS attack in MPSoC to be eligible for the MCDM evaluation process.

1) DESIGN METRICS

Topology. An interconnection scheme used by System-on-Chip designers to localize IP cores of MPSoC platform in an array form with rows and columns denotes by (m×n) (e.g., 2 × 2 and 4 × 4) using NoC links and routers for communication purposes [68], [69].

Routing Algorithm. An NoC communication approach governs the data routing between source and destination IP cores. The routing algorithm plays a significant role in NoC operations used by NoC routers to determine the routing decisions [70]. Most routing algorithms implemented in NoC-based MPSoC are involved in DoS attack scenarios testing deterministic routing algorithms (XY or YX) just because it is common in implementation (simple) and strong to avoid NoC deadlock scenarios.

Location of Implementation. Pre-defined strategy to identify the implementation location (e.g., NoC router or NoC network interface) of countermeasures technique during chip design according to the predicted or proposed DoS threat model or attack scenario as in [45], [54], and [71].

2) PERFORMANCE METRICS

Latency (cycles). A transport latency is the period of time between when a message header is sent into the network at the source node and when a tail flit is received at the destination node. This time is measured by cycles [72].
Frequency (MHz). The clock rate of operating frequency utilized by MPSoC-based IoT IP cores. In order to achieve the highly MPSoC-based IoT security levels during real-time task scheduling, designers assign an operating frequency rate measured by Hertz (e.g., MHz) to enhance the MPSoC resources operating frequency [73].

Area (μm^2) and Power (mW). Both area and power are vital performance metrics for NoC-based MPSoC. The area cost represents the required occupied area for the current buffer design according to the utilized technology. For example, Compromise-NoC (C-NoC) was designed based on (4917 μm^2) as a baseline chip before implementing Fort-NoC as a defense approach against DoS attack [74]. In terms of power, it represents the amount of consumed power due to the typical functional operations of NoC-based MPSoC (the communication among MPSoC IP cores). However, NoC suffers significantly from power consumption induced by switching operations and power leakage of the resources, NoC routers in particular [75].

3) DESIGN OVERHEAD

Area and Power Overhead (%). Additional cost of an area and power consumption rate due to implementing a countermeasure technique against DoS attack from the perspective of chip design. For example, Run-time Latency Auditor for NoCs (RLAN) costs (12.73%) for the area and (9.844%) for power overhead, respectively [76].

Overhead. A scale with three-step (low, average, and high) in comparison to the default MPSoC design overhead without any proposed security (default architecture) [77], [78].

4) DESIGN OVERHEAD

Area and Power Overhead (%). Additional cost of an area and power consumption rate due to implementing a countermeasure technique against DoS attack from the perspective of chip design. For example, Run-time Latency Auditor for NoCs (RLAN) costs (12.73%) for the area and (9.844%) for power overhead, respectively [76].

Overhead. A scale with three-step (low, average, and high) in comparison to the default MPSoC design overhead without any proposed security (default architecture) [77], [78].

5) SECURITY METRICS

Technique Effectiveness. The security guarantees against DoS attacks are rated on a sliding scale from low (very low) to moderate (average) to high (very high) [79].

Evaluation. Three security metrics to evaluate the proposed security approach against DoS attack called:

TABLE 2. DM of DoS A-CTs.

No	Threat Model	Defense Method	Decision Matrix Alternatives	Decision Matrix Criteria													
				Design Metrics			Performance Metrics				Design Overhead			Security Metrics			
			Technique	Topology	Routing Algorithm	location of Implementation	Latency (cycles)	Frequency (MHz)	Area (µm2)	Power (mW)	Area Overhead	Power Overhead	Overhead	Technique Effectiveness	Evaluation	Localization	
1	FD	Additional Validation Checks	Sniffer	8x8	XY	R	99	1.4	1.8	18000	0.033	0.0392	A	H	NC	VCO	
2	FD		Verification Flow	4x4	XY	R	30	2300	35	10.5	0	0.0001	L	A	IL	MNL	
3	FD		SeRA	16x16	XY	R	35.68	1000	10.3	1.7	0.0169	0.0063	L	A	PD	MNL	
4	FD		Secure Model Checkers	8x8	XY	R	28	2000	10.3	1.7	0.011	0.015	L	L	PD	BWT	
5	FD	Traffic Flow Monitoring	Auditor	4x4	XY	NI	60	500	148.349	349	0.1273	0.0984	A	H	NC	MNL	
6	FD		DPU	2x4	XY	NI	0	500	600041.96	72.970	0.256	0.0984	L	H	IL	MNL	
7	TFMD		Runtime-monitor	2x4	YX	R	300	1110	48.386	4.725	0.266	0	L	H	IL	MNL	
8	TFMD		Restart-monitor	2x4	YX	R	300	1110	48.386	4.725	0.22	0	L	H	IL	MNL	
9	TFMD		Intermediate manager	2x4	YX	R	300	1110	48.386	4.725	0.002	0	L	H	IL	MNL	
10	TFMD		Router Auditor	2x4	YX	R	155	1110	48.386	4.725	0.122	0	L	H	IL	MNL	
11	DFD		Collision Point Direction	4x4	YX	R	915.55	200	112187.500	4.174	0.232	0.094	A	A	NC	MNL	
12	DFD		Collision Point Router Detection	4x4	YX	R	915.55	200	107163.700	4.008	0.177	0.05	A	H	NC	MNL	
13	DFD		L.W. DDoS Detection	8x8	XY	R	99	1.4	2.87	0.215	0.06	0.04	H	H	NC	DLC	
14	FD		L.W. DoS Detection	4x4	XY	R	98	1.4	2.87	0.215	0.0593	0.0387	H	H	NC	DLC	
15	FD	Fuzzing and Partitioning	SurfNoC	5x5	XY	R	100	1000	32.7	11.9	0.0262	1.46	A	L	IL	BWT	
16	PCD		Bit Shuffling	4x4	XY	R	15000	1000	41395	16.524	0.212	0.001	A	L	IL	MNL	
17	PCD		Hardened NoC	4x4	XY	R	11.95	500	57514.3	14.1659	0.39	0.13	A	H	IL	MNL	
18	PCD		Threat Detector and L. O.	8x8	XY	R	100	2000	498.3292	227.3749	0.02	0.06	H	H	IL	MNL	

Threat model: Flooding-DoS (FD), Traffic Flow Manipulation-DoS (TFMD), Distributed Flooding-DoS (DFD), Packet Corruption-DoS (PCD). Location of Implementation: Router (R), Network Interface (NI). Architecture Overhead and Technique Effectiveness Scale: High (H), Average (A), Low (L). Evaluation: Number of Collisions (NC), Information Leakage (IL), Probability of Detection (PD). Localization: Maximum Network Latency (MNL), Buffer Waiting Time (BWT), Destination Latency Curve (DLC), Virtual Channel Occupation (VCO).

1) Collision Point: it is a vital security metric from the perspective of a DoS attacker, where at this point, the DoS attack traffic is involved in the sensitive NoC communication path to collide with normal traffic [80].
2) Information Leakage: it is a security metric to evaluate an MPSoC security vulnerability that enables the DoS attacker from leaking confidential information stored in the memory locations to the external world using malicious circuits like Hardware Trojan [81].
3) Probability of Detection: it is the ratio of how many Trojans the technique finds to how many Trojans are in the design as a whole [82].

Localization. Is a security metric based on the Malicious IP (MIP) core location, where the most significant network latency and prior DoS suspect reports determine it. Their solution is less efficient for altering network circumstances since it is based on an experimentally determined threshold [3].

6) DM ALTERNATIVES

Sniffer: is a DoS A-CT based on ML approach to detect and localize malicious IP core [71].

SeRA: Secure Router Architecture***:*** is a DoS A-CT based on discarding or masking infected NoC buffers model to avoid NoC DoS attack [49].

Verification Flow: is a DoS A-CT based on unbounded checking framework to monitor NoC system behaviour to avoid NoC DoS attacks [51].

SMCs: Secure Model Checkers and Switch-to-Switch, are a DoS A-CT based on functionality correctness and control

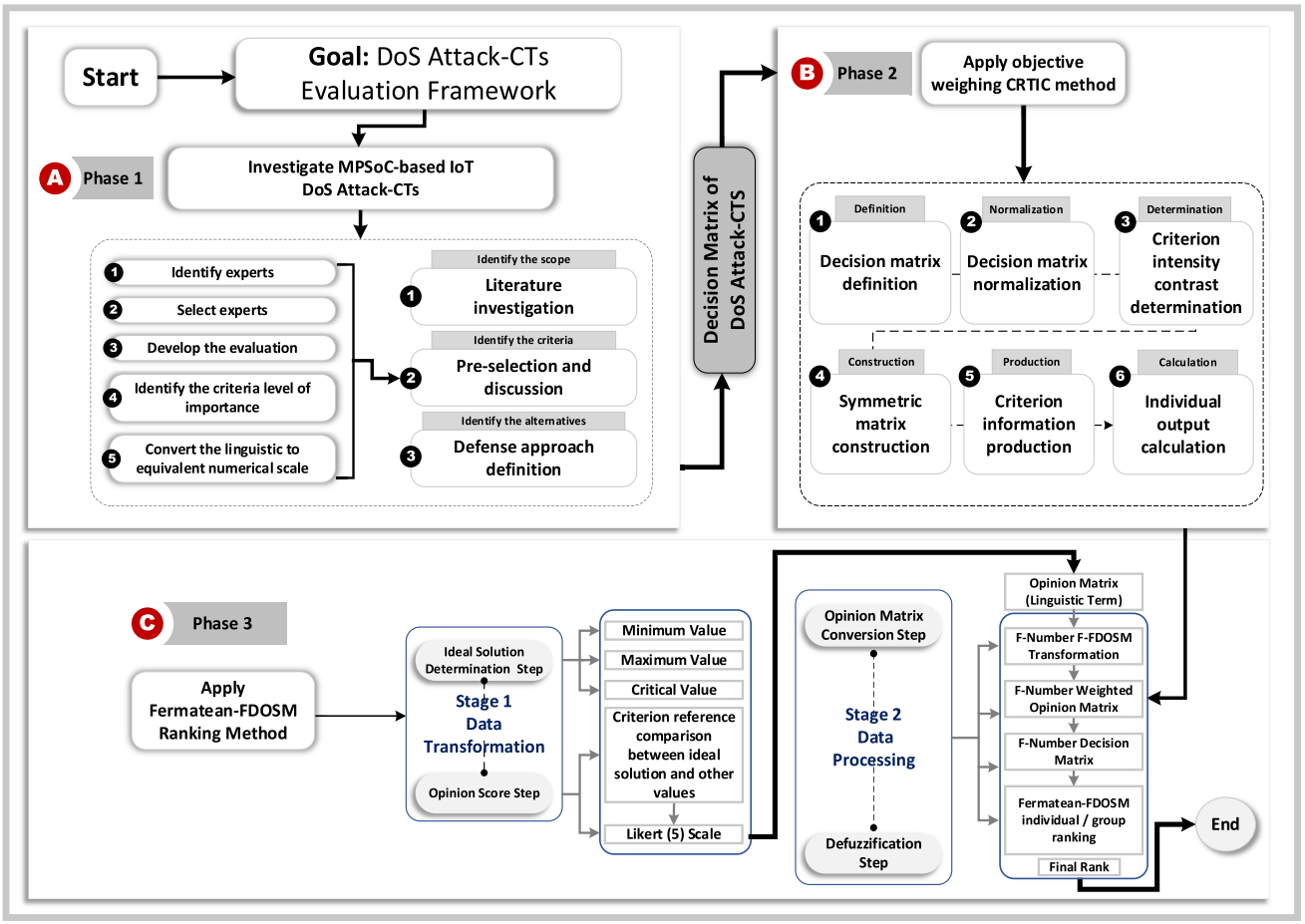

FIGURE 4. Methodology phases.

logic verification methods to detect Hardware Trojan (HT) in MPSoC platforms [83].

Runtime Latency Auditor for NoCs: is a DoS A-CT based on NoC system behavioral monitoring to give an indicate regarding the malicious Rouge NoC third-party IPs insertion scenarios to avoid DoS attack [46].

DPU: Data Protection Unit is DoS A-CT based on memory access filtering to the memory access requests during real-time running scenarios to avoid DoS attacks [84].

Runtime-monitor, Restart-monitor, Intermediate manager, and Auditor: are DoS A-CT based on monitoring methodologies to the routing tables for different NoC router architectures with the aim of detecting DoS attacks [85].

CPDD and CPRD: Collision Point Direction Detection and Collision Point Router Detection: are DoS A-CT based on attacker's packets collied with regular NoC traffic during real-runtime as well as monitor router architectures in order to extend the report of the malicious traffic direction to mitigate and avoid DoS attack [11].

L.W. DDoS Detection: Light-weight DoS Detection, is a DoS A-CT based on NoC traffic monitoring and flagging to detect and localize MIP core to avoid distributed DoS attack [86].

L.W. DoS Detection: Light-weight DoS Detection, is a DoS A-CT based on NoC traffic monitoring and flagging to detect and localize MIP core to avoid DoS attack [87].

SurfNoC: is a DoS A-CT based on NoC latency-reducing methodology to prevent communicating domains from interfering and time division multiplexing (Surf-Scheduling), then prevent communication overhead to avoid DoS attack [88].

Bit Shuffling: is a DoS A-CT based on the bit-shuffling method to mitigate HT effect on NoC system and keep the interactive performance of MPSoC, then mitigate the impact of the DoS attack [44].

Hardened NoC: is a DoS A-CT based on NoC flit integrity check model to ensure and check the potential HT insertion to the NoC system in the design house or third-party system in the integration company to mitigate DoS attack probability [44].

Threat Detector and L.O: Threat Detector and Link Obfuscation, are a DoS A-CT based on a heuristic fault injection detection model to detect HT infect NoC links and L.O. for HT affects mitigation based on switch-to-switch and bit shuffling techniques in order to avoid NoC communication system degradation then avoid DoS attack [87].

B. PHASE 2: CRITERIA WEIGHTING

Phase 2 presents the criteria weighting process of the DM using criteria importance through the inter-criteria correlation (CRITIC) technique, as displayed in FIGURE 4. In order to weight the DM criteria that shown in TABLE 2, there are six stages of the CRITIC technique should be applying [89], as in below:

1) STAGE 1: DM DEFINITION

This stage includes the defined DM in Phases1 based on the set of (m) eligible DoS A-CTs and (n) assessment criteria (i.e., performance). The output of both alternatives and criteria given by DM[d_{ij}], with both i_{th} and j_{th} respectively. See Equation (10).

$$\mathrm{DM} = \left[d_{ij}\right]_{m\times n} = \begin{bmatrix} d_{11} & d_{12} & \ldots & d_{1m} \\ d_{21} & d_{22} & \ldots & d_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ d_{n1} & d_{n2} & \ldots & d_{nm} \end{bmatrix}, \quad (i = 1, 2, \ldots\ldots m; \text{ and } j = 1, 2, \ldots .n) \tag{10}$$

2) STAGE 2: DM NORMALIZATION

Using Equation (11) and ranges between (0 and 1), the DM will normalize to prevent numerical fluctuations of the output values.

$$\bar{d_{ij}} = \frac{d_{ij} - d_j^{\text{worst}}}{d_j^{\text{best}} - d_j^{\text{worst}}} \tag{11}$$

where $\bar{d_{ij}}$ denotes the normalized value of i_{th} alternative of j_{th} criterion. And d_j^{best}, d_j^{worst} denotes the best and worst values of j_{th} criterion.

3) STAGE 3: CONTRAST INTENSITY DETERMINATION

The intensity of the contrast can be determined using the standard deviation of normalized criterion values in the columns d_j. The estimation of the standard deviation of each criterion can be obtained by using Equation (12).

$$\sigma_j = \sqrt{\frac{\sum_{i=1}^{m}\left(\bar{d}_{ij} - \bar{d}_j\right)^2}{m}} \tag{12}$$

where $\bar{d}_j$ is the average output value of j_{th} criterion and (m) represent the number of experiments.

4) STAGE 4: SYMMETRIC MATRIX CONSTRUCTION

In this stage, a symmetric matrix (m × n) will build involving a term r_{jk} to express correlation coefficients such as the criteria's correlation coefficient as in Equation (12).

$$r_{jk} = \frac{\sum_{i=1}^{m}\left(\bar{d_{ij}} - \bar{d_j}\right)\left(\bar{d_{ik}} - \bar{d_k}\right)}{\sqrt{\sum_{i=1}^{m}\left(\bar{d_{ij}} - \bar{d_j}\right)^2 \sum_{i=1}^{m}\left(\bar{d_{ik}} - \bar{d_k}\right)^2}} \tag{13}$$

5) STAGE 5: CRITERION INFORMATION PRODUCTION

This stage depicts the results of Equation (12) as well as Equation (13) and for specifying the criterion information (C_j). As in Equation (14).

$$C_j = \sigma_j \sum_{k=1}^{m} 1 - r_{jk} \tag{14}$$

6) STAGE 6: WEIGHT CALCULATION

This stage shows the weight of individual outputs using criterion information and a normalizing approach, as shown in Equation (15).

$$W_j = \frac{C_j}{\sum_{j=1}^{n} C_j} \tag{15}$$

C. PHASE 3: ALTERNATIVES RANKING

This phase explains the stages of Fermatean-FDOSM used in DoS A-CTs DM ranking, as shown in FIGURE 4. We can summarize the procedure of the Fermatean-FDOSM ranking method in three stages as below:

1) STAGE 1: DATA INPUT

The data input stage is the DM that is built from the intersection of DoS A-CTs criteria, and alternatives see Sec. to get the DoS A-CTs DM formatted based on (A × C) sets of ($A_1, A_2 \ldots\ldots A_m$) alternatives and ($C_1, C_2 \ldots\ldots C_n$) of criteria respectively, as shown below:

$$\mathrm{DM} = \begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{matrix} \begin{bmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \ldots & x_{mn} \end{bmatrix}$$

2) STAGE 2: DATA TRANSFORMATION

This stage includes the following steps:

1) Select the ideal solution among criteria in the form of a 'min, max, critical' range using Equation (16).

$$A^* = \left\{\left(\left(\max_i v_{ij} \mid j \in J\right) \cdot \left(\min_i v_{ij} \mid j \in J\right) \cdot \left(Op_{ij} \in I.J\right) \mid i = 1.2.3.\ldots.m\right)\right\} \tag{16}$$

Fundamentally, (max) refers to the ideal value with the benefit of criteria, (min) refers to the ideal solution, the criteria cost, finally (Op_{jj}) is the critical value, while the ideal value falls between (max) and (min).

2) Identify the panel of experts (refers to the knowledgeable person with a wide range of experience in the research area. These persons are sometimes referred to as 'domain' or ''substantive'' experts in the literature to separate them from ''normative experts'' who are experts in statistics and subjective probability. In the current research, the expert's election approach was based on the analysis of the bibliometrics of all authors and co-authors mentioned in MPSoCs-based IoT security aspects. There are three experts involved in this research.
3) Develop the opinion matrix based on the expert's (decision maker) opinion by comparing the ideal solution

and other values per criterion to produce the expert's opinion matrix with linguistic terms.

4) Transform the expert's opinion matrix to the equivalent numerical matrix using the linguistic Likert scale. The Likert scale suggests that the DoS A-CTs criteria vary in the level of importance that should be assigned to the expert. The aim of using linguistic terms is to determine the level of importance of the criteria assessment procedure. There are five levels of importance from ('NoDifference to HugeDifference') as in below Equation (17) and TABLE 3.

$$Op_{Lang} = \{((\frac{\tilde{v}}{ij} \otimes v_{ij} | j \in J).|\mathrm{i} = 1, 2, 3 \ldots m)\} \quad (17)$$

TABLE 3. Five-point Likert scale, numerical scale, and Fermatean Fuzzy Set (FFS).

Scale of numerical scoring	Scale of linguistic scoring	FFS
1	NoDifference	0.90, 010
2	SlightDifference	0.75, 0.20
3	Difference	0.50, 0.45
4	BigDifference	0.35, 0.60
5	HugeDifference	0.10, 0.90

where $\otimes$ refers to the establishment comparison between ideal solution and alternatives [20].

5) Adopt the opinion matrix that is based on expert opinion, as shown in FIGURE 4, then get the final output of this stage just as transformed to the fuzzy opinion matrix using Fermatean Fuzzy Set (FFS) as below:

$$\mathrm{Op_{Lang}} = \begin{matrix} \\ \mathrm{A_1} \\ \vdots \\ \mathrm{A_m} \end{matrix} \begin{bmatrix} \mathrm{Op_{11}} & \cdots & \mathrm{Op_{1n}} \\ \vdots & \ddots & \vdots \\ \mathrm{Op_{m1}} & \cdots & \mathrm{Op_{mn}} \end{bmatrix}$$

where the term ($\mathrm{Op_{Lang}}$) represent the expert's (decision maker) opinion.

3) STAGE 3: DATA PROCESSING

1) This stage represents the final stage for fuzzy decision matrix ranking, as shown in FIGURE 4.
2) There are two approaches for ranking based on individual and group experts' opinions [20]. Individual decision-making is an approach based on expert opinion to select the best alternative among the others. Group decision-making is an approach based on aggregating the result of multiple decisions from different experts into a unique decision and be calculated using Equation (18).

$$\bar{x} = \frac{1}{n} \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{x_i} \quad (18)$$

where $\bar{x}$ refers to the arithmetic mean.

3) The final rank and score achievement by the defuzzification process for alternatives occurred based on DEFINITION 3 and DEFINITION 5, in addition to use Equation (6) and Equation (9) where the best alternative (countermeasure technique) is associated with a high score.

TABLE 4. DoS A-CTs DM criteria weighting results using CRITIC.

Criteria	Weight
Topology	0.064262871
Routing Algorithm	0.119981974
location of Implementation	0.079152813
Latency	0.058429544
Frequency	0.084775545
Area	0.059000772
Power	0.06335146
Area Overhead	0.078725813
Power Overhead	0.060745744
Overhead	0.069830468
Technique Effectiveness	0.097937732
Evaluation	0.094368089
Localization	0.069437174

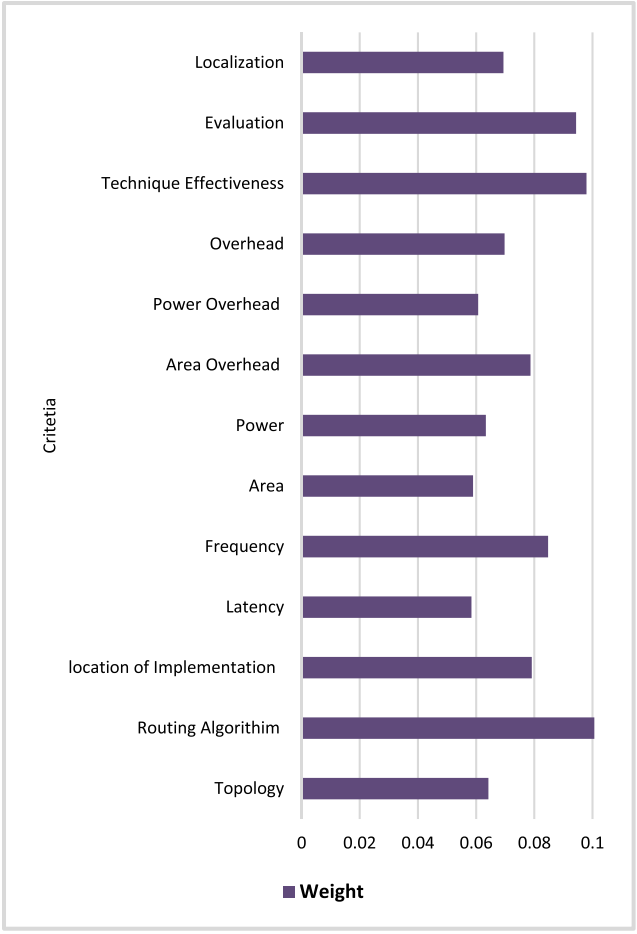

FIGURE 5. Presentation of DoS A-CTs DM criteria weights based on CRITIC method.

IV. DISCUSSION AND RESULTS

This section exhibits the evaluation and classification results of DoS A-CTs to improve security in the context of MPSoCs-based IoT platforms. This section is separated into three

TABLE 5. Opinion matrix of three experts.

Expert 1: Opinion Matrix												
D	ND	D	HD	ND	SD	HD	SD	BD	ND	ND	ND	D
ND	ND	D	SD	HD	SD	D	HD	ND	SD	D	HD	ND
HD	ND	D	D	D	SD	SD	D	D	SD	D	SD	ND
D	ND	D	BD	BD	SD	SD	HD	D	SD	BD	SD	D
ND	ND	ND	BD	SD	D	HD	HD	BD	ND	ND	ND	ND
SD	ND	ND	ND	SD	HD	BD	BD	HD	HD	ND	HD	ND
SD	D	D	HD	D	SD	SD	HD	SD	ND	ND	HD	ND
SD	D	D	HD	D	SD	SD	SD	SD	ND	ND	HD	ND
SD	D	D	HD	D	SD	SD	BD	SD	ND	ND	HD	ND
SD	D	D	HD	D	SD	SD	SD	SD	ND	ND	HD	ND
ND	D	D	HD	SD	HD	SD	SD	SD	ND	D	ND	ND
ND	D	D	HD	SD	HD	ND	BD	HD	ND	ND	ND	ND
D	ND	D	HD	ND	ND	SD	BD	BD	SD	ND	ND	D
ND	ND	D	HD	ND	ND	SD	SD	BD	SD	ND	ND	D
SD	ND	D	HD	D	SD	D	SD	D	SD	BD	HD	D
ND	ND	D	HD	D	BD	D	SD	ND	ND	BD	HD	ND
ND	ND	D	SD	SD	HD	D	ND	SD	BD	ND	HD	ND
D	ND	D	HD	BD	HD	HD	SD	SD	BD	ND	HD	ND
Expert 2: Opinion Matrix												
BD	D	D	HD	BD	D	D	D	BD	D	D	SD	D
SD	D	D	D	HD	D	D	SD	HD	SD	BD	D	D
HD	D	D	D	BD	D	SD	D	D	SD	BD	BD	D
BD	D	D	D	BD	D	SD	D	D	SD	D	BD	D
SD	D	D	D	SD	D	HD	HD	HD	D	D	SD	D
SD	D	D	D	SD	HD	BD	HD	HD	D	D	D	D
SD	D	D	HD	SD	SD	SD	HD	HD	D	D	D	D
SD	D	D	HD	SD	SD	SD	HD	HD	D	D	D	D
SD	D	D	HD	SD	SD	SD	D	HD	D	D	D	D
SD	D	D	HD	SD	SD	SD	BD	HD	D	D	D	D
SD	D	D	HD	BD	HD	SD	SD	BD	D	BD	SD	D
SD	D	D	HD	BD	HD	SD	BD	HD	D	D	SD	D
BD	D	D	HD	BD	D	D	HD	BD	SD	D	SD	SD
SD	D	D	BD	BD	D	D	HD	BD	SD	D	SD	SD
D	D	D	HD	D	SD	BD	SD	D	SD	D	D	BD
SD	D	D	HD	D	HD	BD	D	HD	D	D	D	D

TABLE 5. *(Continued.)* Opinion matrix of three experts.

SD	D	D	D	SD	HD	BD	SD	D	BD	D	D	D
BD	D	D	HD	BD	HD	HD	D	D	BD	D	D	D
Expert 3: Opinion Matrix												
SD	BD	D	BD	HD	BD	D	BD	D	D	D	D	D
BD	BD	D	SD	HD	SD	SD	D	D	D	D	HD	D
D	BD	D	D	SD	BD	BD	SD	D	D	D	SD	D
SD	BD	D	SD	D	BD	BD	D	SD	D	HD	SD	D
BD	BD	D	SD	D	D	HD	HD	HD	D	D	D	D
BD	BD	D	BD	D	HD	BD	HD	HD	D	D	HD	D
BD	D	D	HD	SD	D	D	HD	D	D	D	HD	D
BD	D	D	HD	SD	D	D	HD	D	D	D	HD	D
BD	D	D	HD	SD	D	D	D	D	D	D	HD	D
BD	D	D	HD	SD	D	D	HD	D	D	D	HD	D
BD	D	D	HD	HD	HD	D	HD	HD	D	D	D	D
BD	D	D	HD	HD	HD	D	HD	D	D	D	D	D
SD	BD	D	BD	BD	BD	BD	BD	D	D	D	D	D
BD	BD	D	BD	HD	BD	BD	BD	D	D	D	D	D
D	BD	D	BD	D	SD	D	HD	D	D	HD	HD	D
BD	BD	D	HD	D	HD	SD	HD	D	D	HD	HD	D
BD	BD	D	SD	BD	HD	SD	D	D	D	D	HD	D
SD	BD	D	BD	D	HD	HD	D	D	D	D	HD	D

The linguistic five levels scale of importance, NoDifference (ND), SlightDifference (SD), Difference (D), BigDifference (BD), and HugeDifference (HD). See TABLE 3.

sub-sections. Firstly, the section "Criteria Weighting Results" presented the CRITIC method results of weighting and adopted criteria weights; specifically, the panel of three experts (decision makers) opinions to be converted using a mathematical approach to achieve the final weight results. Secondly, the section "Ranking results" show the rank of DoS A-CTs DM alternatives based on individual and group decision-making Fermatean-FDOSM are then presented. Finally, the section "Validation" validates the final results of the ranking process.

A. CRITERIA WEIGHTING RESULTS

This section presents the DoS A-CTs DM criteria weighting results using CRITIC method as developed in Section III. As we mentioned, the CRITIC approach has six steps to be applied to compute the DM criteria weights. The obtained weights after applying Equation (11) to normalize the DM into the interval of (0 to 1) then using Equation (12) to determine the intensity of the contrast using the standard deviation of normalized criterion values. Moreover, Equation (13) was

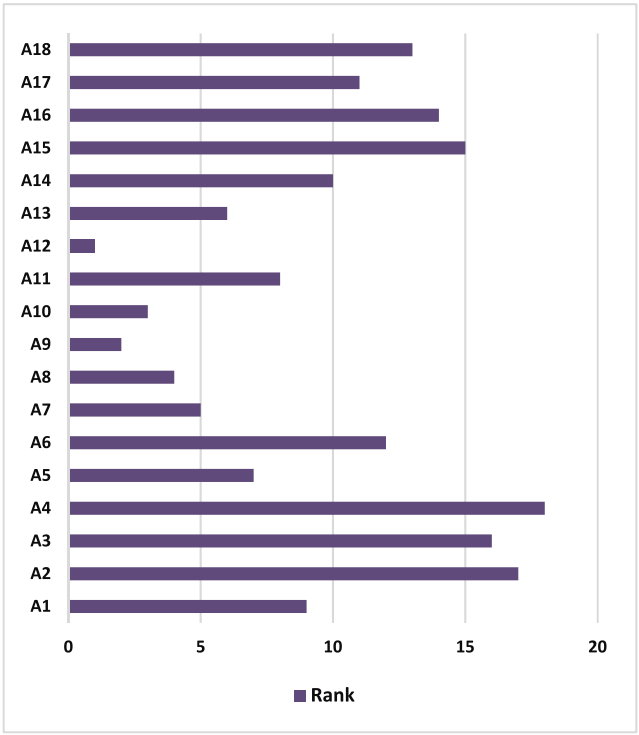

FIGURE 6. Graph of group decision-making ranking.

utilized after obtaining a symmetric matrix to express the criteria's correlation coefficient. Furthermore, Equation (14) and Equation (15) were used for criterion information production and weight calculation for every thirteen criteria, respectively.

Both TABLE 4 and FIGURE 5 are depicts weighting results, which indicate the vital (significant) variation of thirteen criteria of DoS A-CTs based on the CRITIC technique. The NoC routing algorithm received the highest weight as the first vital criterion, followed by the technique effectiveness as a security metric to evaluate a DoS attacks on MPSoCs-based IoT platforms as a second vital criterion. the size, power, NoC architecture overhead, and localization have received the same importance as the lowest importance criteria.

Consequently, the NoC area and latency received the lowest weight as an important criterion. Besides, the size, power, NoC architecture overhead, and localization have received the same importance as the lowest importance criteria. The final evaluation results can be obtained by using the Fermatean-FDOSM method as described in the next section; realistically, in order, these CRITIC weight values must be feed to Fermatean-FDOSM to calculate the final rank of the eighteen DoS A-CTs.

B. ALTERNATIVES RANKING RESULTS

The results and discussion in this section relate to evaluating the DoS A-CTs based on Fermatean-FDOSM individual and group of experts' opinions. Each expert records his opinion using the data of DM in (TABLE 2), to determine the ideal solution of each criterion, then apply Equation (16) and Equation (17) to compare the ideal solution with other values per criterion or each alternative using linguist terms. Using the Likert five scale approach, the three experts presented the opinion matrix as illustrated in TABLE 5.

The resulting three experts' opinion matrices will be converted to a fuzzy opinion matrix using the Fermatean fuzzy set (FFS) by applying Equation (2). In order to aggregate the FFS values of each alterative, there are two approaches, as mentioned in Section III:

1) Individual decision-making can be calculated using Equation (4) and Equation (5), and the results are shown in TABLE 6. The first rank

TABLE 6. DoS A-CTs ranking results based on individual decision-making F-FDOSM.

Alternative		Expert 1		Expert 2		Expert 3	
		Score	Rank	Score	Rank	Score	Rank
Sniffer	A1	0.003689	3	0.002073	16	0.002234	8
Verification Flow	A2	0.002388	11	0.002143	14	0.00122	18
SeRA	A3	0.002565	9	0.001315	17	0.002044	10
Secure Model Checkers	A4	0.002192	13	0.001201	18	0.001618	14
Auditor	A5	0.003906	2	0.002351	13	0.002124	9
DPU	A6	0.003325	5	0.002473	12	0.001422	17
Runtime-monitor	A7	0.001933	18	0.003974	3	0.003277	3
Restart-monitor	A8	0.002138	14	0.003974	3	0.003277	3
Intermediate manager	A9	0.001954	17	0.004329	1	0.003338	2
Router Auditor	A10	0.002138	14	0.003995	2	0.003277	3
Collision Point Direction	A11	0.002359	12	0.002969	7	0.002888	6
Collision Point Router Detection	A12	0.002725	7	0.003692	5	0.003483	1
L.W. DDoS Detection	A13	0.003569	4	0.00305	6	0.002451	7
L.W. DoS Detection	A14	0.003914	1	0.002116	15	0.001907	11
SurfNoC	A15	0.002088	16	0.00257	10	0.001444	16
Bit Shuffling	A16	0.002534	10	0.002723	9	0.001521	15
Hardened NoC	A17	0.003282	6	0.002772	8	0.001726	12
Threat Detector and L.O.	A18	0.002626	8	0.002555	11	0.001694	13

TABLE 7. DoS A-CTs ranking results based on group decision-making F-FDOSM.

Alternative		Score	Rank
Sniffer	A1	0.002665	9
Verification Flow	A2	0.001917	17
SeRA	A3	0.001974	16
Secure Model Checkers	A4	0.00167	18
Auditor	A5	0.002793	7
DPU	A6	0.002407	12
Runtime-monitor	A7	0.003062	5
Restart-monitor	A8	0.00313	4
Intermediate manager	A9	0.003207	2
Router Auditor	A10	0.003137	3
Collision Point Direction	A11	0.002739	8
Collision Point Router Detection	A12	0.0033	1
L.W. DDoS Detection	A13	0.003023	6
L.W. DoS Detection	A14	0.002646	10
SurfNoC	A15	0.002034	15
Bit Shuffling	A16	0.00226	14
Hardened NoC	A17	0.002594	11
Threat Detector and L. O.	A18	0.002292	13

2) From the perspective of the first expert is given to 'Light Weight DoS Detection' countermeasure technique, while the first rank from the second expert point of view is for 'Intermediate Manager' countermeasure technique, whereas the third expert has appointed 'Collision Point Router Detection' is the first ranked countermeasure technique. From what aforementioned, there was a verity regarding individual decision-making approach results. To reach the fair consensus using a group decision-making approach, the three experts were able to come to a mutual agreement, and their findings are summarized in TABLE 7.
3) Group decision-making can be calculated using Equation (18), and the results are shown in TABLE 7. The 'Collision Point Router Detection (A12)' countermeasure technique is earned the first rank (rank 1) as the best defense against MPSoC-based IoT DoS attacks.

V. VALIDATION

The group decision-making approach prioritization results of DoS A-CTs were used to prove that the Fermatean FDOSM outputs were correct. This method has been used by researchers to prove that their results are correct [90], [91]. For numerical verification, the group decision-making of DoS A-CTs with each design and security metrics were put into different groups. The number of groups or CTs in each group did not change the validation results. To verify the group decision-making prioritizing results, the following steps were taken: (1) combining the opinion matrices by adding up each one; (2) sorting a DoS A-CTs based on the group decision-making results in the combined opinion matrix; (3) dividing the sorted CTs into six equal groups; and (4) using Equation (18) to find the arithmetic mean ($\bar{x}$) for each group across all eighteen CTs as displayed in TABLE 8. The six groups' ranking results were systematically allocated between the countermeasure techniques of DoS attack categories. TABLE 8 shows that the mean value of the 1st Group followed by 2nd Group and so on for the other groups. Thus, the suggested Fermatean-FDOSM that utilized is valid and ranked the groups systematically.

TABLE 8. Validation of group decision-making approach ranking results.

Groups	*Mean*
1st Group	0.003215
2nd Group	0.003072
3rd Group	0.002732
4th Group	0.002549
5th Group	0.002195
6th Group	0.001854

VI. CONCLUSION

The evaluation of the DoS A-CTs in terms of MPSoCs-based IoT, which is based on the new MCDM method called Fermatean-FDOSM, was conducted. The methodology of this study included three phases, as illustrated in FIGURE 4. The first phase is DoS A-CTs decision matrix construction. The second phase consists of six steps of DM criteria weighting using the CRITIC method, and the third phase includes the steps of DM alternative ranking using the Fermatean-FDOSM method. The main contribution of this study is the proposed evaluation framework to tackle the challenge of selecting the most potent countermeasure technique against DoS attacks in terms of MPSoCs-based IoT. The validation of evaluation results is performed utilizing an arithmetic mean statistical approach.

REFERENCES

[1] L. Daoud and N. Rafla, "Efficient mitigation technique for black hole router attack in network-on-chip," *Microprocessors Microsyst.*, vol. 94, Oct. 2022, Art. no. 104658, doi: 10.1016/j.micpro.2022.104658.
[2] L. S. Indrusiak, J. Harbin, C. Reinbrecht, and J. Sepúlveda, "Side-channel protected MPSoC through secure real-time networks-on-chip," *Microprocessors Microsyst.*, vol. 68, pp. 34–46, Jul. 2019, doi: 10.1016/j.micpro.2019.04.004.
[3] M. Sinha, S. Gupta, S. S. Rout, and S. Deb, "Sniffer: A machine learning approach for DoS attack sniffer: A machine learning approach for DoS attack localization in NoC-based SoCs," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 278–291, Jun. 2021.
[4] A. C. Sant'Ana, H. Medina, and F. G. Moraes, "Security vulnerabilities and countermeasures in MPSoCs," *IEEE Design Test*, vol. 38, no. 4, pp. 70–77, Aug. 2021, doi: 10.1109/MDAT.2021.3049710.
[5] G. Sharma, G. Bousdras, S. Ellinidou, O. Markowitch, J.-M. Dricot, and D. Milojevic, "Exploring the security landscape: NoC-based MPSoC to cloud-of-chips," *Microprocessors Microsyst.*, vol. 84, Jul. 2021, Art. no. 103963, doi: 10.1016/j.micpro.2021.103963.
[6] L. Zhang, X. Wang, Y. Jiang, M. Yang, T. Mak, and A. K. Singh, "Effectiveness of HT-assisted sinkhole and blackhole denial of service attacks targeting mesh networks-on-chip," *J. Syst. Archit.*, vol. 89, pp. 84–94, Sep. 2018, doi: 10.1016/j.sysarc.2018.07.005.
[7] L. Daoud, "Secure network-on-chip architectures for MPSoC: Overview and challenges," in *Proc. IEEE 61st Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2018, pp. 542–543, doi: 10.1109/MWSCAS.2018.8623831.

[8] J. Sepúlveda, A. Zankl, D. Flórez, and G. Sigl, "Towards protected MPSoC communication for information protection against a malicious NoC," *Proc. Comput. Sci.*, vol. 108, pp. 1103–1112, Jan. 2017, doi: 10.1016/j.procs.2017.05.139.
[9] R. Manju, A. Das, J. Jose, and P. Mishra, "SECTAR: Secure NoC using trojan aware routing," in *Proc. 14th IEEE/ACM Int. Symp. Netw. Chip (NOCS)*, Sep. 2020, pp. 1–8, doi: 10.1109/NOCS50636.2020.9241711.
[10] H. Ali, U. U. Tariq, J. Hardy, X. Zhai, L. Lu, Y. Zheng, F. Bensaali, A. Amira, K. Fatema, and N. Antonopoulos, "A survey on system level energy optimisation for MPSoCs in IoT and consumer electronics," *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100416, doi: 10.1016/j.cosrev.2021.100416.
[11] C. Chaves, S. Azad, T. Hollstein, and J. Sepúlveda, "DoS attack detection and path collision localization in NoC-based MPSoC architectures," *J. Low Power Electron. Appl.*, vol. 9, no. 1, p. 7, Feb. 2019, doi: 10.3390/jlpea9010007.
[12] K. Goossens, J. Dielissen, and A. Radulescu, "Æthereal network on chip: Concepts, architectures, and implementations," *IEEE Design Test Comput.*, vol. 22, no. 5, pp. 414–421, May 2005, doi: 10.1109/MDT.2005.99.
[13] D. Bertozzi and L. Benini, "Xpipes: A network-on-chip architecture for gigascale systems-on-chip," *IEEE Circuits Syst. Mag.*, vol. 4, no. 2, pp. 18–31, Sep. 2004, doi: 10.1109/MCAS.2004.1330747.
[14] W. Wolf, A. A. Jerraya, and G. Martin, "Multiprocessor system-on-chip (MPSoC) technology," *IEEE Trans. Comput.-Aided Design Integr.*, vol. 27, no. 10, pp. 1701–1713, Oct. 2008, doi: 10.1109/TCAD.2008.923415.
[15] J. Zhou, J. Sun, P. Cong, Z. Liu, X. Zhou, T. Wei, and S. Hu, "Security-critical energy-aware task scheduling for heterogeneous real-time MPSoCs in IoT," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 745–758, Jul. 2020, doi: 10.1109/TSC.2019.2963301.
[16] D. Diakoulaki, G. Mavrotas, and L. Papayannakis, "Determining objective weights in multiple criteria problems: The critic method," *Comput. Oper. Res.*, vol. 22, no. 7, pp. 763–770, 1995, doi: 10.1016/0305-0548(94)00059-H.
[17] S. Gaur, S. Dosapati, and A. Tawalare, "Stakeholder assessment in construction projects using a CRITIC-TOPSIS approach," *Built Environ. Project Asset Manage.*, vol. 12, no. 6, Aug. 2022, doi: 10.1108/BEPAM-10-2021-0122.
[18] G. Silvius and R. Schipper, "Planning project stakeholder engagement from a sustainable development perspective," *Administ. Sci.*, vol. 9, no. 2, p. 46, Jun. 2019, doi: 10.3390/admsci9020046.
[19] Ž. Stević, D. Pamučar, A. Puška, and P. Chatterjee, "Sustainable supplier selection in healthcare industries using a new MCDM method: Measurement of alternatives and ranking according to COmpromise solution (MARCOS)," *Comput. Ind. Eng.*, vol. 140, Feb. 2020, Art. no. 106231, doi: 10.1016/j.cie.2019.106231.
[20] M. M. Salih, B. B. Zaidan, and A. A. Zaidan, "Fuzzy decision by opinion score method," *Appl. Soft Comput.*, vol. 96, Nov. 2020, Art. no. 106595, doi: 10.1016/j.asoc.2020.106595.
[21] O. S. Albahri, A. A. Zaidan, A. S. Albahri, H. A. Alsattar, R. Mohammed, U. Aickelin, G. Kou, F. Jumaah, M. M. Salih, A. H. Alamoodi, B. B. Zaidan, M. Alazab, A. Alnoor, and J. R. Al-Obaidi, "Novel dynamic fuzzy decision-making framework for COVID-19 vaccine dose recipients," *J. Adv. Res.*, vol. 37, pp. 147–168, Mar. 2022, doi: 10.1016/j.jare.2021.08.009.
[22] M. M. Salih, O. S. Albahri, A. A. Zaidan, B. B. Zaidan, F. M. Jumaah, and A. S. Albahri, "Benchmarking of AQM methods of network congestion control based on extension of interval type-2 trapezoidal fuzzy decision by opinion score method," *Telecommun. Syst.*, vol. 77, no. 3, pp. 493–522, Jul. 2021, doi: 10.1007/s11235-021-00773-2.
[23] M. S. Al-Samarraay, M. M. Salih, M. A. Ahmed, A. A. Zaidan, O. S. Albahri, D. Pamucar, H. A. AlSattar, A. H. Alamoodi, B. B. Zaidan, K. Dawood, and A. S. Albahri, "A new extension of FDOSM based on Pythagorean fuzzy environment for evaluating and benchmarking sign language recognition systems," *Neural Comput. Appl.*, vol. 34, no. 6, pp. 4937–4955, Mar. 2022, doi: 10.1007/s00521-021-06683-3.
[24] A. H. Alamoodi, R. T. Mohammed, O. S. Albahri, S. Qahtan, A. A. Zaidan, H. A. Alsattar, A. S. Albahri, U. Aickelin, B. B. Zaidan, M. J. Baqer, and A. N. Jasim, "Based on neutrosophic fuzzy environment: A new development of FWZIC and FDOSM for benchmarking smart e-tourism applications," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3479–3503, Aug. 2022, doi: 10.1007/s40747-022-00689-7.
[25] U. S. Mahmoud, "A methodology of DASs benchmarking to support industrial community characteristics in designing and implementing advanced driver assistance systems within vehicles," Universiti Pendidikan Sultan Idris, Perak, Malaysia, Tech. Rep., 2021.
[26] M. S. Al-Samarraay, A. A. Zaidan, O. S. Albahri, D. Pamucar, H. A. AlSattar, A. H. Alamoodi, B. B. Zaidan, and A. S. Albahri, "Extension of interval-valued Pythagorean FDOSM for evaluating and benchmarking real-time SLRSs based on multidimensional criteria of hand gesture recognition and sensor glove perspectives," *Appl. Soft Comput.*, vol. 116, Feb. 2022, Art. no. 108284, doi: 10.1016/j.asoc.2021.108284.
[27] A. S. Albahri, O. S. Albahri, A. A. Zaidan, A. Alnoor, H. A. Alsattar, R. Mohammed, A. H. Alamoodi, B. B. Zaidan, U. Aickelin, M. Alazab, S. Garfan, I. Y. Y. Ahmaro, and M. A. Ahmed, "Integration of fuzzy-weighted zero-inconsistency and fuzzy decision by opinion score methods under a q-rung orthopair environment: A distribution case study of COVID-19 vaccine doses," *Comput. Standards Interface*, vol. 80, Mar. 2022, Art. no. 103572, doi: 10.1016/j.csi.2021.103572.
[28] M. A. Alsalem, H. A. Alsattar, A. S. Albahri, R. T. Mohammed, O. S. Albahri, A. A. Zaidan, A. Alnoor, A. H. Alamoodi, S. Qahtan, B. B. Zaidan, U. Aickelin, M. Alazab, and F. M. Jumaah, "Based on T-spherical fuzzy environment: A combination of FWZIC and FDOSM for prioritising COVID-19 vaccine dose recipients," *J. Infection Public Health*, vol. 14, no. 10, pp. 1513–1559, Oct. 2021, doi: 10.1016/j.jiph.2021.08.026.
[29] T. Senapati and R. R. Yager, "Fermatean fuzzy sets," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 2, pp. 663–674, Feb. 2020, doi: 10.1007/s12652-019-01377-0.
[30] R. R. Yager, "Pythagorean membership grades in multicriteria decision making," *IEEE Trans. Fuzzy Syst.*, vol. 22, no. 4, pp. 958–965, Aug. 2014, doi: 10.1109/TFUZZ.2013.2278989.
[31] K. T. Atanassov, "Intuitionistic fuzzy sets," *Fuzzy Sets Syst.*, vol. 20, pp. 87–96, Aug. 1986, doi: 10.1016/S0165-0114(86)80034-3.
[32] J. S, "Ordering of interval-valued fermatean fuzzy sets and its applications," *Expert Syst. Appl.*, vol. 185, Dec. 2021, Art. no. 115613, doi: 10.1016/j.eswa.2021.115613.
[33] G. Shahzadi, F. Zafar, and M. A. Alghamdi, "Multiple-attribute decision-making using fermatean fuzzy Hamacher interactive geometric operators," *Math. Problems Eng.*, vol. 2021, pp. 1–20, Jun. 2021, doi: 10.1155/2021/5150933.
[34] V. Simić, I. Ivanović, V. Dorić, and A. E. Torkayesh, "Adapting urban transport planning to the COVID-19 pandemic: An integrated fermatean fuzzy model," *Sustain. Cities Soc.*, vol. 79, Apr. 2022, Art. no. 103669, doi: 10.1016/j.scs.2022.103669.
[35] J. Aldring and D. Ajay, "MABAC method for assessment of cyber security technologies under fermatean fuzzy sets," in *Evolution in Computational Intelligence*. Cham, Switzerland: Springer, 2022, pp. 441–450.
[36] M. Kabak, S. Aydın, and A. Aktaş, "Internet of Things fermatean fuzzy CRITIC testing procedure for new normal," in *Proc. Int. Conf. Intell. Fuzzy Syst.*, 2022, pp. 649–655.
[37] M. K. Saraji, D. Streimikiene, and G. L. Kyriakopoulos, "Fermatean fuzzy CRITIC-COPRAS method for evaluating the challenges to industry 4.0 adoption for a sustainable digital transformation," *Sustainability*, vol. 13, no. 17, p. 9577, Aug. 2021.
[38] C. Cao and M. Zhang, "Credit risk evaluation of quantum communications listed companies in China based on fermatean fuzzy TOPSIS," *Proc. Comput. Sci.*, vol. 199, pp. 361–368, Jan. 2022.
[39] L. Daoud and N. Rafla, "Efficient mitigation technique for black hole router attack in network-on-chip," *Microprocessors Microsyst.*, vol. 94, Oct. 2022, Art. no. 104658, doi: 10.1016/j.micpro.2022.104658.
[40] C. G. Chaves, S. P. Azad, T. Hollstein, and J. Sepúlveda, "DoS attack detection and path collision localization in NoC-based MpsoC architectures," *J. Low Power Electron. Appl.*, vol. 9, no. 1, pp. 1–20, 2019, doi: 10.3390/jlpea9010007.
[41] F. Khalid, S. R. Hasan, O. Hasan, and F. Awwad, "Runtime hardware trojan monitors through modeling burst mode communication using formal verification," *Integration*, vol. 61, pp. 62–76, Mar. 2018, doi: 10.1016/j.vlsi.2017.11.003.
[42] S. Charles, Y. Lyu, and P. Mishra, "Real-time detection and localization of DoS attacks in NoC based SoCs," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, pp. 1160–1165, doi: 10.23919/DATE.2019.8715009.
[43] S. Charles, Y. Lyu, and P. Mishra, "Real-time detection and localization of distributed DoS attacks in NoC-based SoCs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4510–4523, Dec. 2020, doi: 10.1109/TCAD.2020.2972524.

[44] M. K. Jyv, A. K. Swain, S. Kumar, S. R. Sahoo, and K. Mahapatra, "Run time mitigation of performance degradation hardware trojan attacks in network on chip," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2018, pp. 738–743, doi: 10.1109/ISVLSI.2018.00139.

[45] J. Frey and Q. Yu, "A hardened network-on-chip design using runtime hardware trojan mitigation methods," *Integration*, vol. 56, pp. 15–31, Jan. 2017, doi: 10.1016/j.vlsi.2016.06.008.

[46] R. Js, D. M. Ancajas, K. Chakraborty, and S. Roy, "Runtime detection of a bandwidth denial attack from a rogue network-on-chip," in *Proc. 9th Int. Symp. Netw. Chip*, Sep. 2015, pp. 1–8, doi: 10.1145/2786572.2786580.

[47] T. Boraten, D. DiTomaso, and A. K. Kodi, "Secure model checkers for network-on-chip (NoC) architectures," in *Proc. 26th Ed., Great Lakes Symp. (VLSI)*, May 2016, pp. 45–50, doi: 10.1145/2902961.2903032.

[48] T. Boraten and A. K. Kodi, "Mitigation of denial of service attack with hardware trojans in NoC architectures," in *Proc. IEEE Int. Parallel Distrib. Process. Symp. (IPDPS)*, May 2016, pp. 1091–1100, doi: 10.1109/IPDPS.2016.59.

[49] N. Prasad, R. Karmakar, S. Chattopadhyay, and I. Chakrabarti, "Run-time mitigation of illegal packet request attacks in networks-on-chip," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2017, pp. 2–5, doi: 10.1109/ISCAS.2017.8050633.

[50] D. Fang, H. Li, J. Han, and X. Zeng, "Robustness analysis of mesh-based network-on-chip architecture under flooding-based denial of service attacks," in *Proc. IEEE 8th Int. Conf. Netw., Archit. Storage*, Jul. 2013, pp. 178–186, doi: 10.1109/NAS.2013.29.

[51] J. Sepulveda, D. Aboul-Hassan, G. Sigl, B. Becker, and M. Sauer, "Towards the formal verification of security properties of a network-on-chip router," in *Proc. IEEE 23rd Eur. Test Symp. (ETS)*, May 2018, pp. 1–6, doi: 10.1109/ETS.2018.8400692.

[52] L. Fiorin, G. Palermo, and C. Silvano, "A security monitoring service for NoCs," in *Proc. 6th IEEE/ACM/IFIP Int. Conf. Hardw./Softw. Codesign Syst. Synth. (CODES/ISSS)*, Oct. 2008, pp. 197–202, doi: 10.1145/1450135.1450180.

[53] R. Js, D. M. Ancajas, K. Chakraborty, and S. Roy, "Runtime detection of a bandwidth denial attack from a rogue network-on-chip," in *Proc. 9th Int. Symp. Net. Chip*, Sep. 2015, pp. 1–8, doi: 10.1145/2786572.2786580.

[54] A. K. Biswas, S. K. Nandy, and R. Narayan, "Router attack toward NoC-enabled MPSoC and monitoring countermeasures against such threat," *Circuits, Syst., Signal Process.*, vol. 34, no. 10, pp. 3241–3290, Oct. 2015, doi: 10.1007/s00034-015-9980-0.

[55] L. A. Zadeh, "Fuzzy sets," *Inf. Control*, vol. 8, no. 3, pp. 338–353, Jun. 1965, doi: 10.1016/S0019-9958(65)90241-X.

[56] D. Simić, I. Kovačević, V. Svirčević, and S. Simić, "50 years of fuzzy set theory and models for supplier assessment and selection: A literature review," *J. Appl. Log.*, vol. 24, pp. 85–96, Nov. 2017, doi: 10.1016/j.jal.2016.11.016.

[57] T. Senapati and R. R. Yager, "Fermatean fuzzy weighted averaging/geometric operators and its application in multi-criteria decision-making methods," *Eng. Appl. Artif. Intell.*, vol. 85, pp. 112–121, Oct. 2019, doi: 10.1016/j.engappai.2019.05.012.

[58] T. Senapati and R. R. Yager, "Some new operations over fermatean fuzzy numbers and application of fermatean fuzzy WPM in multiple criteria decision making," *Informatica*, vol. 30, no. 2, pp. 391–412, Jan. 2019.

[59] S. B. Aydemir and S. Y. Gunduz, "Fermatean fuzzy TOPSIS method with dombi aggregation operators and its application in multi-criteria decision making," *J. Intell. Fuzzy Syst.*, vol. 39, no. 1, pp. 851–869, Jul. 2020, doi: 10.3233/JIFS-191763.

[60] A. R. Mishra and P. Rani, "Multi-criteria healthcare waste disposal location selection based on fermatean fuzzy WASPAS method," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2469–2484, Oct. 2021, doi: 10.1007/s40747-021-00407-9.

[61] S. Gül, "Fermatean fuzzy set extensions of SAW, ARAS, and VIKOR with applications in COVID-19 testing laboratory selection problem," *Expert Syst.*, vol. 38, no. 8, pp. 1–16, Dec. 2021, doi: 10.1111/exsy.12769.

[62] A. R. Mishra, P. Rani, and K. Pandey, "Fermatean fuzzy CRITIC-EDAS approach for the selection of sustainable third-party reverse logistics providers using improved generalized score function," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 1, pp. 295–311, Jan. 2022, doi: 10.1007/s12652-021-02902-w.

[63] P. Rani and A. R. Mishra, "Fermatean fuzzy Einstein aggregation operators-based MULTIMOORA method for electric vehicle charging station selection," *Expert Syst. Appl.*, vol. 182, Nov. 2021, Art. no. 115267, doi: 10.1016/j.eswa.2021.115267.

[64] M. K. Saraji, D. Streimikiene, G. L. Kyriakopoulos, and M. Tvaronaviciene, "Fermatean fuzzy CRITIC-COPRAS method for evaluating the challenges to industry 4.0 adoption for a sustainable digital transformation," Kaunas Fac., Vilnius Univ., Kaunas, Lithuania, Tech. Rep., 2021, doi: 10.3390/su13179577.

[65] D. Liu, Y. Liu, and L. Wang, "Distance measure for fermatean fuzzy linguistic term sets based on linguistic scale function: An illustration of the TODIM and TOPSIS methods," *Int. J. Intell. Syst.*, vol. 34, no. 11, pp. 2807–2834, Nov. 2019, doi: 10.1002/int.22162.

[66] H. A. Alsattar, S. Qahtan, R. T. Mohammed, A. A. Zaidan, O. S. Albahri, G. Kou, A. H. Alamoodi, A. S. Albahri, B. B. Zaidan, M. S. Al-Samarraay, R. Q. Malik, and A. N. Jasim, "Integration of FDOSM and FWZIC under homogeneous fermatean fuzzy environment: A prioritization of COVID-19 patients for mesenchymal stem cell transfusion," *Int. J. Inf. Technol. Decis. Making*, pp. 1–41, Sep. 2022.

[67] M. M. Salih, Z. T. Al-Qaysi, M. L. Shuwandy, M. A. Ahmed, K. F. Hasan, and Y. R. Muhsen, "A new extension of fuzzy decision by opinion score method based on Fermatean fuzzy: A benchmarking COVID-19 machine learning methods," *J. Intell. Fuzzy Syst.*, vol. 43, pp. 3549–3559, 2022, doi: 10.3233/JIFS-220707.

[68] B. Halavar, U. Pasupulety, and B. Talawar, "Extending BookSim2.0 and HotSpot6.0 for power, performance and thermal evaluation of 3D NoC architectures," *Simul. Model. Pract. Theory*, vol. 96, Nov. 2019, Art. no. 101929, doi: 10.1016/j.simpat.2019.101929.

[69] A. A. J. Al-Hchaimi, W. N. Flayyih, F. Hashim, M. S. Rusli, and F. Z. Rokhani, "Review of 3D networks-on-chip simulators and plugins," in *Proc. IEEE Asia Pacific Conf. Postgraduate Res. Microelectron. Electron. (PrimeAsia)*, Nov. 2021, pp. 17–20, doi: 10.1109/PrimeAsia51450.2021.9701472.

[70] A. B. Gabis and M. Koudil, "NoC routing protocols—Objective-based classification," *J. Syst. Archit.*, vols. 66–67, pp. 14–32, May 2016, doi: 10.1016/j.sysarc.2016.04.011.

[71] M. Sinha, S. Gupta, S. S. Rout, and S. Deb, "Sniffer: A machine learning approach for DoS attack localization in NoC-based SoCs," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 278–291, Jun. 2021, doi: 10.1109/JETCAS.2021.3083289.

[72] P. P. Pande, C. Grecu, M. Jones, A. Ivanov, and R. Saleh, "Performance evaluation and design trade-offs for network-on-chip interconnect architectures," *IEEE Trans. Comput.*, vol. 54, no. 8, pp. 1025–1040, Aug. 2005, doi: 10.1109/TC.2005.134.

[73] J. Zhou, J. Sun, P. Cong, Z. Liu, X. Zhou, T. Wei, and S. Hu, "Security-critical energy-aware task scheduling for heterogeneous real-time MPSoCs in IoT," *IEEE Trans. Services Comput.*, vol. 13, no. 4, pp. 745–758, Jul. 2020, doi: 10.1109/TSC.2019.2963301.

[74] D. M. Ancajas, K. Chakraborty, and S. Roy, "Fort-NoCs: Mitigating the threat of a compromised NoC," in *Proc. 51st Annu. Design Autom. Conf. Design Autom. Conf. (DAC)*, 2014, pp. 1–6, doi: 10.1145/2593069.2593144.

[75] K. Lee, S.-J. Lee, and H.-J. Yoo, "Low-power network-on-chip for high-performance SoC design," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 14, no. 2, pp. 148–160, Feb. 2006, doi: 10.1109/TVLSI.2005.863753.

[76] R. Js, D. M. Ancajas, K. Chakraborty, and S. Roy, "Runtime detection of a bandwidth denial attack from a rogue network-on-chip," in *Proc. 9th Int. Symp. Net. Chip*, Sep. 2015, pp. 1–8, doi: 10.1145/2786572.2786580.

[77] R. Fernandes, C. Marcon, R. Cataldo, and J. Sepulveda, "Using smart routing for secure and dependable NoC-based MPSoCs," *IEEE/ACM Trans. Netw.*, vol. 28, no. 3, pp. 1158–1171, Jun. 2020, doi: 10.1109/TNET.2020.2979372.

[78] K. Patel, S. Parameswaran, and R. G. Ragel, "Architectural frameworks for security and reliability of MPSoCs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 9, pp. 1641–1654, Sep. 2011, doi: 10.1109/TVLSI.2010.2053856.

[79] M. D. Grammatikakis, K. Papadimitriou, P. Petrakis, A. Papagrigoriou, G. Kornaros, I. Christoforakis, and M. Coppola, "Security effectiveness and a hardware firewall for MPSoCs," in *Proc. IEEE IEEE Int. Conf High Perform. Comput. Commun. 6th Int. Symp. Cyberspace Saf. Secur. 11th Int. Conf. Embedded Softw. Syst (HPCC,CSS,ICESS)*, Aug. 2014, pp. 1032–1039, doi: 10.1109/HPCC.2014.173.

[80] C. G. Chaves, S. P. Azad, T. Hollstein, and J. Sepulveda, "A distributed DoS detection scheme for NoC-based MPSoCs," in *Proc. IEEE Nordic Circuits Syst. Conf. (NORCAS): NORCHIP Int. Symp. Syst. Chip (SoC)*, Oct. 2018, pp. 1–6, doi: 10.1109/NORCHIP.2018.8573524.

[81] A. Das, G. Memik, J. Zambreno, and A. Choudhary, "Detecting/preventing information leakage on the memory bus due to malicious hardware," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*. IEEE, Mar. 2010, pp. 861–866.
[82] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014, doi: 10.1109/JPROC.2014.2335155.
[83] T. Boraten, D. DiTomaso, and A. K. Kodi, "Secure model checkers for network-on-chip (NoC) architectures," in *Proc. 26th Ed., Great Lakes Symp. (VLSI)*, May 2016, pp. 45–50, doi: 10.1145/2902961.2903032.
[84] L. Fiorin, G. Palermo, S. Lukovic, V. Catalano, and C. Silvano, "Secure memory accesses on networks-on-chip," *IEEE Trans. Comput.*, vol. 57, no. 9, pp. 1216–1229, Sep. 2008, doi: 10.1109/TC.2008.69.
[85] A. K. Biswas, S. K. Nandy, and R. Narayan, "Router attack toward NoC-enabled MPSoC and monitoring countermeasures against such threat," *Circuits, Syst., Signal Process.*, vol. 34, no. 10, pp. 3241–3290, Oct. 2015, doi: 10.1007/s00034-015-9980-0.
[86] S. Charles, Y. Lyu, and P. Mishra, "Real-time detection and localization of distributed DoS attacks in NoC-based SoCs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4510–4523, Dec. 2020, doi: 10.1109/TCAD.2020.2972524.
[87] T. Boraten and A. Kodi, "Mitigation of Hardware Trojan based denial-of-service attack for secure NoCs," *J. Parallel Distrib. Comput.*, vol. 111, pp. 24–38, Jan. 2018, doi: 10.1016/j.jpdc.2017.06.014.
[88] H. M. G. Wassel, Y. Gao, J. K. Oberg, T. Huffmire, R. Kastner, F. T. Chong, and T. Sherwood, "SurfNoC: A low latency and provably non-interfering approach to secure networks-on-chip," in *Proc. 40th Annu. Int. Symp. Comput. Archit.*, Jun. 2013, pp. 583–594, doi: 10.1145/2485922.2485972.
[89] G. C. Patel, "Experimental modeling and optimization of surface quality and thrust forces in drilling of high-strength Al 7075 alloy: CRITIC and meta-heuristic algorithms," *J. Brazilian Soc. Mech. Sci. Eng.*, vol. 43, no. 5, pp. 1–21, May 2021. Accessed: Sep. 20, 2022.
[90] O. S. Albahri, A. A. Zaidan, M. M. Salih, B. B. Zaidan, M. A. Khatari, M. A. Ahmed, A. S. Albahri, and M. Alazab, "Multidimensional benchmarking of the active queue management methods of network congestion control based on extension of fuzzy decision by opinion score method," *Int. J. Intell. Syst.*, vol. 36, no. 2, pp. 796–831, Feb. 2021, doi: 10.1002/int.22322.
[91] K. H. Abdulkareem, N. Arbaiy, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, M. A. Alsalem, and M. M. Salih, "A new standardisation and selection framework for real-time image dehazing algorithms from multi-foggy scenes based on fuzzy delphi and hybrid multi-criteria decision analysis methods," *Neural Comput. Appl.*, vol. 33, no. 4, pp. 1029–1054, Feb. 2021, doi: 10.1007/s00521-020-05020-4.

AHMED ABBAS JASIM AL-HCHAIMI received the B.Tech. degree in computer engineering and the M.Tech. degree in computer networks and information security engineering from the School of Information Technology (SIT), from Jawaharlal Nehru Technological University, Hyderabad, India, in 2011 and 2014, respectively. He is currently pursuing the Ph.D. degree in computer and embedded systems engineering with the Faculty of Engineering, University of Putra Malaysia, Serdang, Selangor, Malaysia. From 2014 to 2016, he was a Research Assistant at the Electrical and Electronic Engineering Department, College of Engineering, University of ThiQar. From 2017 to 2018, he joined Lukoil Middle East, the leading operator of the giant West-Qurna-2 oil field, as an IT Network Engineer in the IT and T Department. He is currently a Lecturer with the Electromechanical System Engineering Department, ThiQar Technical College, Southern Technical University, Iraq, Basra. His research interests include on-chip communication security as well as multiprocessors system-on-chip (MPSoCs) security enhancement using MCDM theory and ML.

NASRI BIN SULAIMAN (Member, IEEE) received the bachelor's degree in electronics and computer engineering from Universiti Putra Malaysia (UPM), Malaysia, in 1994, the master's degree in microelectronics system design from the University of Southampton, U.K., in 1999, and the Ph.D. degree in adaptive hardware from The University of Edinburgh, U.K., in 2007. He is currently an Associate Professor with the Department of Electrical and Electronic Engineering, Faculty of Engineering, UPM. He is currently working on a variety of research projects such as High Performance Hardware Implementation of a Multi-Objective Genetic Algorithm which is funded through the Research University Grant Scheme (RUGS) of Universiti Putra Malaysia (UPM), as well as Crest Factor Reduction and Digital Pre-distortion Implementation in Orthogonal Frequency Division Multiplexing (OFDM) Systems, funded by the Ministry of Science, Technology and Innovation (MOSTI). His research interests include evolutionary algorithms, digital signal processing, digital communications, and low power VLSI designs.

MOHD AMRALLAH BIN MUSTAFA (Senior Member, IEEE) received the B.Eng. degree in electrical and electronics and the M.Sc. degree in control and automation engineering from Universiti Putra Malaysia, Malaysia, in 2000 and 2007, respectively, and the Ph.D. degree in engineering from Shizuoka University, Japan, in 2013. He is currently a Senior Lecturer with the Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Putra Malaysia.

MOHD NAZIM BIN MOHTAR (Senior Member, IEEE) received the B.Eng. degree (Hons.) in medical engineering and the Ph.D. degree in biomedical engineering from the University of Surrey, U.K., in 2006 and 2013, respectively. In 2014, he was a Visiting Researcher at the Department of Electrical Engineering, University of Cambridge, attached to The HeteroGenesys Laboratory. He is currently a Senior Lecturer with the Department of Electrical and Electronic Engineering, University Putra Malaysia. His research interests include sensors, lab on a chip (LOC) device, and renewable energy.

SITI LAILATUL BINTI MOHD HASSAN received the bachelor's degree (Hons.) in electrical engineering from Universiti Teknologi MARA, Malaysia, in 2007, the Master of Engineering Science degree from the University of New South Wales, Australia, in 2009, and the Ph.D. degree from Universiti Putra Malaysia, in 2020. She has been working as a Lecturer with the College of Engineering, Universiti Teknologi MARA, since 2009. Her major areas of interest are embedded systems and integrated circuit design. Her current research interests include Verilog coding and FPGA system implementation.

YOUSIF RAAD MUHSEN received the Bachelor of Computer Science degree from the College of Science, Al-Mustansiriya University, Iraq, in 2008, and the Master of Computer Science degree from the Saint Petersburg State University of Transportation, Russia, in 2016. He is currently pursuing the Ph.D. degree in computer science with the Faculty of Computer Science and Information Technology, University Putra Malaysia (UPM), Selangor, Malaysia.