Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

A comprehensive evaluation approach for efficient countermeasure techniques against timing side-channel attack on MPSoC-based IoT using multi-criteria decision-making methods

Ahmed Abbas Jasim Al-Hchaimi [a,b,*], Nasri Bin Sulaiman [a,c,*], Mohd Amrallah Bin Mustafa [c], Mohd Nazim Bin Mohtar [c], Siti Lailatul Binti Mohd Hassan [d], Yousif Raad Muhsen [e]

[a] Department of Computer and Embedded Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, Serdang, Selangor 43400, Malaysia
[b] Department of Electromechanical Systems Engineering, ThiQar Technical College, Southern Technical University, Basra 61 61001, Iraq
[c] Department of Electrical and Electronic Engineering, Faculty of Engineering, Universiti Putra Malaysia, Serdang, Selangor 43400, Malaysia
[d] Department of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Shah Alam, Selangor 40450, Malaysia
[e] Center of Information Technology, College of Engineering, University of Wasit, Kut FRXQ+RC4, Iraq

ARTICLE INFO

Article history:
Received 20 November 2022
Revised 8 January 2023
Accepted 7 May 2023
Available online 18 May 2023

Keywords:
NoC Security
Multi-Processor System-On-Chip (MPSoC)
Timing Side-channel Attack
Multi-criteria Decision Making
CRITIC
Fermatean Fuzzy Set (FFS)

ABSTRACT

Context: Timing side-channel attack countermeasure techniques (TSCA-CTs) evaluation is a multi-criteria decision-making (MCDM) problem based on different MPSoCs of IoT platform architectures, performance, and design overhead. Therefore, the Fermatean by fuzzy decision opinion score method (F-FDOSM) for prioritizing the powerful countermeasure technique against timing side-channel attack is the best approach because it employs the most efficient MCDM ranking technique. Nonetheless, the FDOSM method needs to weigh 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 TSCA-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 seven defense approaches (e.g., Gossip and SER router) based on ten criteria (e.g., number of malicious IP cores, number of routers, power, latency… etc.). Then, the decision matrix 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 throughput (packet/clock) is the highest weight criterion, whereas latency (clock/cycle) is the less weight criterion. (2) The Fermatean-FDOSM-based group ranking shows that the Adaptive routing countermeasure technique is the highest score alternative compared to the Combined with separate interface hybrid approach. (3) The TSCA-CTs priority ranks were subjected to a systematic ranking that was confirmed by strong correlation results throughout ten criterion weight values. A comparison with recent studies confirmed the feasibility of the proposed framework.
Conclusion: The outcomes of this study are anticipated to give particular knowledge and direction to those who want to do decision theory-based MPSoCs-based IoT and NoC communication security research.

* Corresponding authors.
E-mail addresses: al-hchaimi.ahmed@student.upm.edu.my, ahmed.alhchaimi@stu.edu.iq (A.A.J. Al-Hchaimi), nasri_sulaiman@upm.edu.my (N.B. Sulaiman), amrallah@upm.edu.my (M.A.B. Mustafa), nazim@upm.edu.my (M.N.B. Mohtar), sitilailatul@uitm.edu.my (S.L.B. Mohd Hassan), yousif@uowasit.edu.iq (Y.R. Muhsen).

https://doi.org/10.1016/j.eij.2023.05.005
1110-8665/

1. Introduction

1.1. Motivation

The tremendous advancement in computational systems have resulted in adopting of parallel architectures using Multiprocessor System-On-Chips (MPSoCs) [1]. Particularly the IoT is based on MPSoCs devices that have become more and more complicated as well as powerful and thus are linked together through a 5G network [2].

However, due to their extensive use in critical applications and resource sharing, MPSoCs have become prone to hardware and software attacks that might 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) [4,5]. This fact also offers an extreme threat to semiconductor suppliers and ultimate MPSoCs customers, including mobile communications crucial applications and cyber-infrastructure like aerospace agencies, military nuclear weaponry, and medical electronics [6,7] Given the current circumstances, it is not only necessary but also difficult to research several defensive approaches and Countermeasure techniques (CTs) in order to mitigate the possible risks to data security presented via what are known as side-channel attacks, specifically TSCAs.

1.2. Challenges

Because of the growing attention shown by academia and industry, the research on Timing Side-channel attack countermeasure techniques (TSCA-CTs) in the context of MPSoCs-based IoT remains scarce in the literature. Most academic journal articles have concentrated on the techniques of MPSoCs IP core cache hierarchies or Network-on-Chip (NoC) vulnerabilities from the perspective of designers and engineers [2,8]. Some studies have focused on the MPSoCs communication system routing protocols and routers aspects, highlighting the necessity of being the proposed defense techniques compatible with MPSoC design constraints [9–11] or investigating the appropriate countermeasure technique for MPSoC in real runtime [3,12,13]. We provide a methodology that helps facilitate both design and implementation aspects of selecting powerful countermeasure techniques against TSCAs in the context of MPSoCs-based IoT alternatives.

In general, choosing the suitable criteria to assess the countermeasure technique against TSCA 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 TSCAs 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 useful tools to aid experts in making the right decision by giving more robust and precise results.

1.3. Objectives

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

(i) Providing an efficient and systematic technique to the problem of selecting powerful countermeasure techniques against TSCAs in the context of MPSoCs-based IoT.
(ii) Offering an accurate formal representation for the often vague or unclear subjective assessments of experts.
(iii) Giving a solid example demonstrating the relevance and effectiveness of the suggested countermeasure techniques against TSCAs in the context of MPSoCs-based IoT with ambiguous and unclear information.
(iv) Gaining insights to practitioners and academics about decision support systems in the embedded system security domain.

1.4. Contribution and significance

In order to evaluate and rank MPSoCs-based IoT countermeasure techniques, the current work seeks to propose an integrated CRITIC approach with Fermatean-FDOSM for decision-making under uncertainty. In a nutshell, this article mostly contributes the following:

(i) This study fills the gap in evaluating the different approaches of defense against TSCAs in the context of MPSoCs-based IoT.
(ii) This study for the first time proposes a decision matrix for TSCA-CTs includes ten criterion and seven alternatives.
(iii) This study, for the first-time integrated CRITIC + Fermatean-FDOSM.
(iv) This study, for the first time, employs the CRITIC method to wight TSCA-CTs criteria.
(v) This study, for the first time, utilizes the Fermatean-FDOSM method with MPSoCs-based IoT countermeasure techniques decision matrix to find the most efficient countermeasure technique.
(vi) In addition, this study uses the individual and group approach of ranking to extract the right decision in terms of selecting the most potent countermeasure technique against TSCA in the context of MPSoCs.

In terms of the study significance:

- As far as we know, no study has been done in the scope of timing side-channel attacks in terms of MPSoCs-based IoT to weight and evaluate the countermeasure techniques, criteria, and alternatives.
- The general significance of this study is to provide a new approach that can rapidly and efficiently model expert assessments and rank alternatives while considering confusing and unclear facts as well as the degree of confidence of the experts.
- Additionally, this work contributes to the body of knowledge on methodologies for evaluating TSCAs countermeasure techniques. This case study makes a significant contribution in this regard, considering the uniqueness of the proposed approach and the focus on defense mechanism selection issues in recent research.
- The case study's findings show the suggested method's applicability, effectiveness, and adaptability, which may be used to address the powerful countermeasure techniques against TSCAs selection issues for MPSoCs-based IoT with comparable features.

The reminder of this study is organized as: Sec. 2, presented state-of-the-art literature review in terms of TSCAs in the context of MPSoCs-based IoT, studies on FDOSM, and CRITIC methods. Sect. 3 illustrated a comprehensive overview of the suggested methodology. In addition, Sec. 4, addressed the discussion of study results produced by applying CRITIC criteria weighting and Fermatean FDOSM alternatives ranking methods. Finally, Sec. 5 concluded this study.

2. Literature review

The literature review is organized into three subsections. First, we review some of the current research lines and studies on MPSoCs of IoT TSCAs and countermeasure techniques against TSCAs especially in the context of IP core caches and NoC. The second part focus on FDOSM. The last section focuses on some recent studies in terms of FFSs.

2.1. Studies on TSCAs in the context of MPSoCs-based IoT

Side-Channel Attacks (SCAs) are very effective methods of attack whose primary goal is to get sensitive information by evaluating logical e.g., timing, or physical e.g., power dissipation, or electromagnetic emanation impacts created during typical system runtime as shown in Fig. 1. Where all these attacks almost share the most common characteristics in terms of compromising the secret information from the perspective of MPSoCs-based IoT platforms and defenses such as attack categories, threat models, and countermeasure techniques [11]. As Timing Side-channel Attacks (TSCAs) is the primary focus of this study, cache hierarchies of MPSoC IP cores and NoC are the most targeted components [15]. Nowadays, TSCAs pose a significant threat to the semiconductor industry since they may be conducted entirely in software and often remotely [5]. Furthermore, because these adversaries merely observe the system's behaviour, they are challenging to detect or recognize. According to Subodha and Carreon et al. [16,17], security attacks in embedded systems in software can be classified as intrusive or physical, as well as SCAs.

In addition, Sepúlveda et al. [2,18] mentioned approximately eighty percent of all attacks on embedded systems are software-based. Attacks on software may emerge from malicious implemented programs or operating systems such as firmware. TSCAs software-based attacks include Malware, denial-of-service, worms, viruses, trojans, critical information extraction, spyware, and hijacking [19].

2.2. Timing side-channel attack (TSCA) threat model and categories

2.2.1. TSCA threat model

Timing side-channel attackers perform their attacks using a specific framework called Threat Model in Fig. 2 to complete the attack process on MPSoCs-based IoT. The general framework of the threat model for TSCA on MPSoCs includes the following steps: Infection, Observation, and Analysis, as shown in Fig. 2. In the Infection step, the adversary infects the MPSoC pre-identified IP core with malicious software such as Malware. For the observation step, the adversaries observe the MPSoC IP cores' cache hierarchies access locations. According to [20–22], the observation occurs in terms of the access location of performing the sensitive operation such as RSA modulo multiplications of two large numbers. Whereas, in [10,22,23], the observation process has two major actions, Prime and Probe, respectively, when the cryptography IP cores perform the AES algorithm.

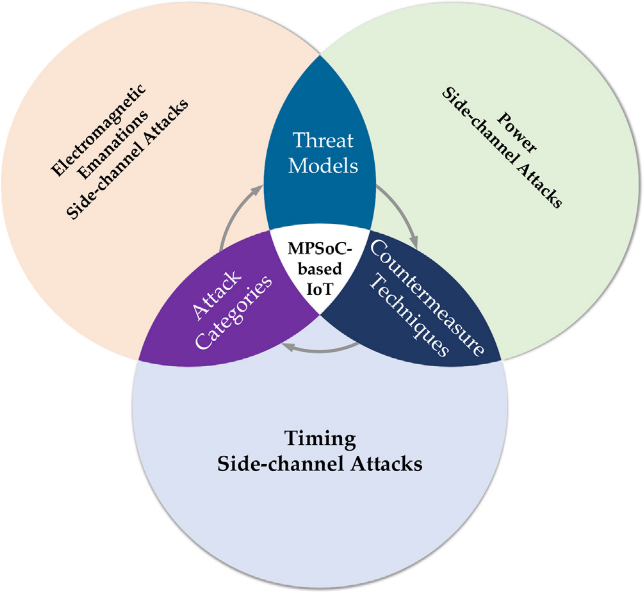


Fig. 1. Side-channel attacks in terms of MPSoCs-based IoT.

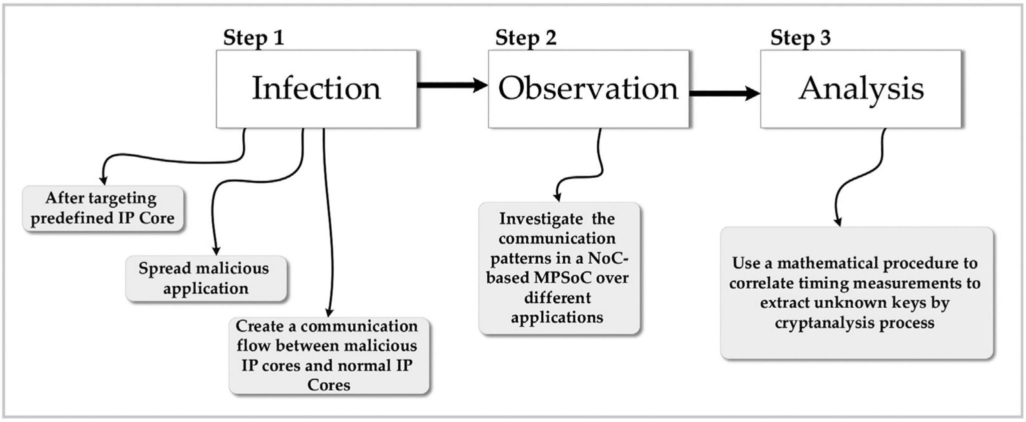
On the one hand, the Prime procedure performing overwrites the cache memory locations just to guarantee there are no lookup tables of AES operations before the attack starts. On the other hand, the probe procedure checks cache access patterns in the AES operation execution. Accordingly, the analyses step is post-processing in which the attackers use special algorithm to correlate the collected throughput samples to reveal the secret keys.

2.2.2. TSCA categories

TSCA attack strategy in terms of MPSoCs can be categorized into Single Timing Attacks (STA) and Distributed Timing Attacks (DTA) based on the number of malicious IP cores participating in the attack process [9,10]. Both STA and DTA share the same approach characteristics in terms of TSCA threat model steps infection, observation, and analysis, as displayed in Fig. 3. STA is an attack strategy in which the attacker uses a single malicious IP to grant access and control the system. According to [9,21,22,24], STA assumes that two applications on the system are running concurrently as shown in Fig. 4(a). Where (S) is the sensitive application and (A) is the attacker. When (S) involves carrying out a cryptographic operation such as RSA that uses a secret key. On each data request, the cache is integrated into the running IP core checks to see if the data is stored on it. If it does, a hit is made, and the data is sent to the IP core. Otherwise, there is a miss, and access to main memory (D) is required, requiring the sensitive traffic to utilize the NoC. (S) starts a communication with the memories (D). Sensitive traffic is the collection of communication flows from (S) to (D). Additionally, (A) is continually injecting packets into the NoC linking (S) and (D), and the goal is to keep track of the (S-D) set of connections [10]. DTA is an improved methodology from STA. According to [2,10,23], multiple IP cores can be infected to increase the attack's impact. The DTA reduces the processing and storage needs of malicious IPs as compared to STA. In DTA, the infected IP cores can be categorized into Injectors (I) and Observers (O), as shown in Fig. 4(a). On the one hand, (I) is responsible for injecting data at high data rates into the NoC to raise the traffic delays of the attacked path. On the other hand, (O) injects at lower data rates and samples the delay of their packets to collect the throughput traces of the attacked path. As a result, both STA and DTA share the same characteristics in terms of the threat model, as shown in Fig. 4(b). In addition, MPSoC design necessitates security solutions to avoid possible threats to sensitive information, threaten data integrity and potentially cause data damage.

2.2.3. TSCA-CTs

Traffic partitioning and route randomization are the two main categories to countermeasure TSCAs in the context of MPSoCs [25,9]. The traffic partitioning goal is to prevent packets from securing applications from interfering with non-secure applications. Non-secure application latency and throughput become independent of certain application traffic behaviour. Statically dividing resources of NoC (link bandwidth, buffer, etc.) spatially or temporally may do this. Sub-optimal solutions might degrade performance.



After targeting predefined IP Core

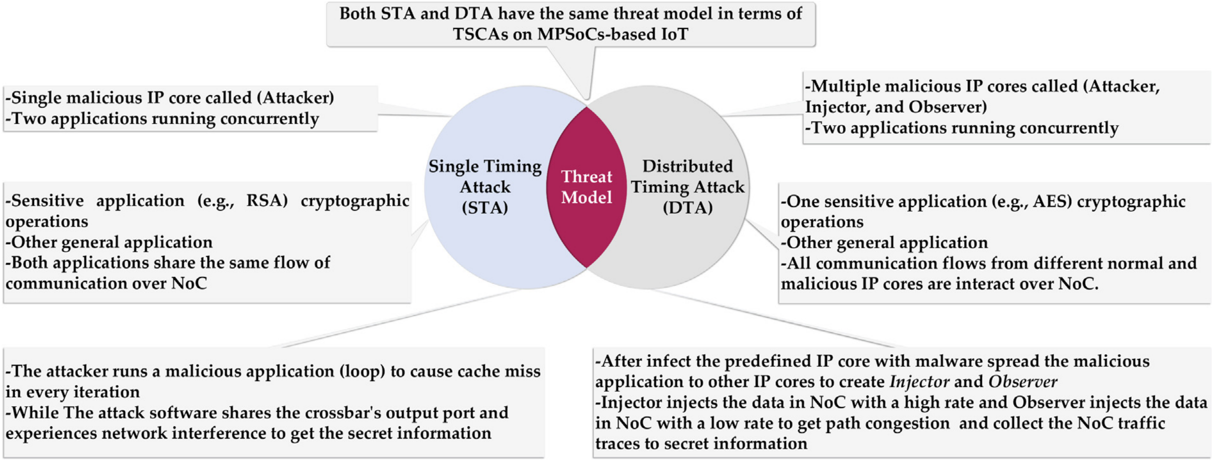
Spread malicious application

Create a communication flow between malicious IP cores and normal IP Cores

Investigate the communication patterns in a NoC-based MPSoC over different applications

Use a mathematical procedure to correlate timing measurements to extract unknown keys by cryptanalysis process

Fig. 2. An illustrative diagram of TSCA threat model in the context of MPSoC-based IoT.



Both STA and DTA have the same threat model in terms of TSCAs on MPSoCs-based IoT

-Single malicious IP core called (Attacker)
-Two applications running concurrently

-Sensitive application (e.g., RSA) cryptographic operations
-Other general application
-Both applications share the same flow of communication over NoC

-The attacker runs a malicious application (loop) to cause cache miss in every iteration
-While The attack software shares the crossbar's output port and experiences network interference to get the secret information

-Multiple malicious IP cores called (Attacker, Injector, and Observer)
-Two applications running concurrently

-One sensitive application (e.g., AES) cryptographic operations
-Other general application
-All communication flows from different normal and malicious IP cores are interact over NoC.

-After infect the predefined IP core with malware spread the malicious application to other IP cores to create *Injector* and *Observer*
-Injector injects the data in NoC with a high rate and Observer injects the data in NoC with a low rate to get path congestion and collect the NoC traffic traces to secret information

Fig. 3. An illustrative diagram to prove both STA and DTA share the exact characteristics of the TSCA threat model.

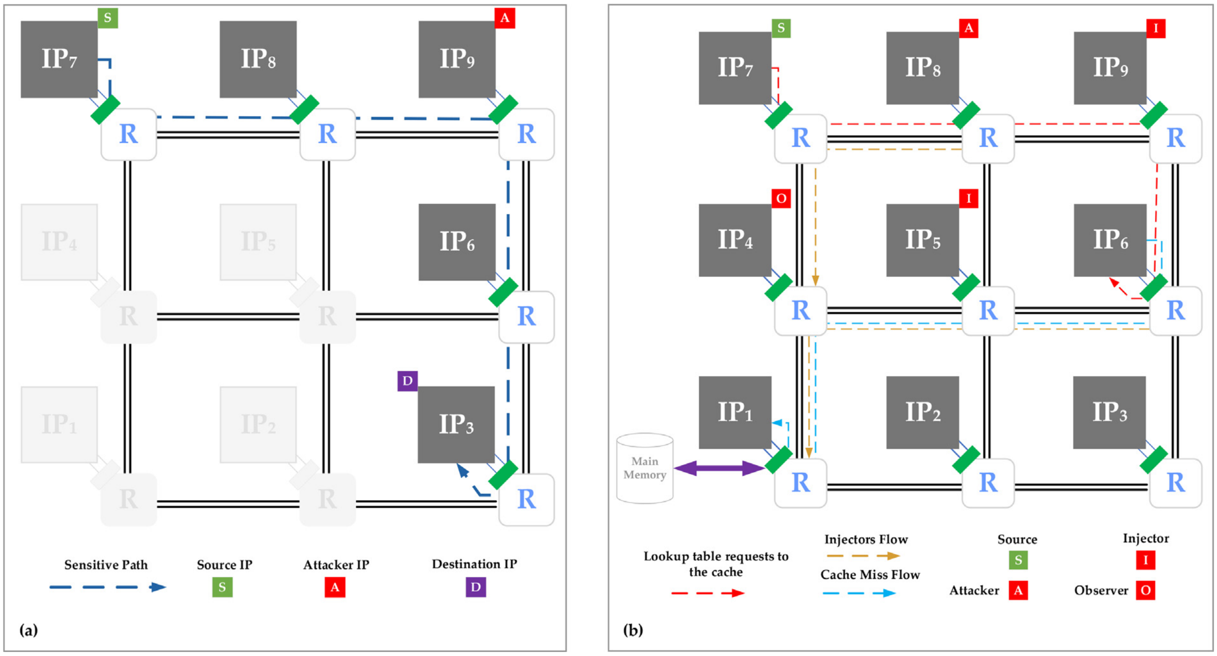


Fig. 4. (a) STA and (b) DTA approach in context of MPSoC.

In contrast, the route randomization countermeasure technique is based on two stages. The first stage is to detect the TSCA attack by monitoring the bandwidth and sending an alert notification (message) in case of any security threat. The second stage is the alert message activates the protection mechanism, which subsequently modifies the routing protocols to redirect packets away from the sensitive path containing the malicious IP cores [10,26,23]. These methods incur a performance overhead. In addition, the software and hardware necessary to manage the countermeasure add significant area and power requirements. The SER router referred to in reference [21] shows a 9% area (μm2) and 8% power (mW) overhead in comparison with the base router design without countermeasure. In addition, the Gossip router presented in reference [10] displays 21.16% area (μm2) and 16.2% power (mW) in comparison with a typical router.

Despite all of these defensive systems and their extraordinary robustness, it is impossible to offer a unified front in which a single countermeasure approach system has all of the ideal attributes. Instead, diverse countermeasure techniques will demonstrate significant differences in their respective aspects, including attack techniques and the number of malicious IP cores, NoC architecture cost and performance metrics of proposed countermeasure techniques, the overhead of implemented countermeasures techniques, and countermeasure technique security [2,10,20,21,23,24,27,28]. This is a challenging occurrence; however, it may be handled by analyzing various identification systems to choose the best acceptable way. Therefore, it is nearly hard to find a perfect match between all the works offered for TSCA's countermeasure strategies based on a '*cloud*' information approach. Hence, a comparison between the real-time TSCAs countermeasure techniques based on a certain perspective (i.e., security, performance, power, and area) is unfair because of these differences. In addition, some of these countermeasure techniques are implemented using simulation software, whereas others are implemented on real hardware. For example, the Prime + Probe attack and countermeasure, i.e., the Gossip Router scenario in [23] has been implemented on real hardware FPGA (ARM Cortex-A9 core) whereas, other countermeasure techniques such as Separate interface Hybrid (CSH), Separate Hybrid (SH), Combined, and Combined Hybrid (CH) routers are implemented using Bluespec System Verilog (BSV) for design and simulation purposes [9,29]. Consequently, not everyone will agree on the significance of these values, resulting in distinct criteria values and varied significance.

2.3. Why choosing CRITIC

The CRITIC is a robust criterion weighting method proposed by Diakoulaki (1995). CRITIC is an objective approach for calculating the weight of criteria, including a degree of conflict and contrast in the main structure of the decision-making problem. CRITIC belongs to the class of correlation techniques and is based on the analytical calculation of a decision matrix to specify the information included in the criteria used to assess the alternatives. CRITIC methodology consists of six stages, the standard deviation of normalized criterion values by columns and the correlation coefficients of all pairs of columns are used to determine the criteria contrast [30–33].

2.4. Why choosing FDOSM

Mahmood [34] recently presented a new MCDM technique called the Fuzzy decision by opinion score method (FDOSM). A stable and effective MCDM method in a fuzzy environment is proposed by FDOSM. The FDOSM strategy is built on a three-stage process that includes "data input," "transformation," and "processing." Individual and group decision-making tools are used in FDOSM. The experts (decision-makers) may use the FDOSM technique, which is based on the notion of ideal solutions, to determine which value is the best and how it compares to other values using the same criteria. Thus, a distinct mathematical operation is required to get the final rank and choose the best option from a collection of feasible choices. The use of FDOSM in conjunction with fuzzy methods and competing criteria has shown promising results [35–41].

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

2.5. Why working with Fermatean fuzzy sets

Yager formulated the theory of Fermatean fuzzy sets (FFSs) [42] in (2020). FFSs are an unique generalization of both Pythagorean fuzzy sets (PFSs) [43] and Intuitionistic fuzzy sets (IFSs) [44]. FFSs provide a more comprehensive picture of fuzzy sets, since the sum of the cubes of the membership and non-membership degrees is in the unit interval. They make it easier for professionals to provide their views on membership ratings [45–47]. FFSs are more flexible and efficient than IFSs and PyFSs when it comes to handling information with a degree of uncertainty. The current study used FFSs to represent decision-making uncertainties in the context of adapting TSCAs countermeasure techniques, allowing for a more precise evaluation of the importance of main and sub-criteria, an accurate evaluation of experts' reputations, and an effective assessment of explored alternatives. Models based on FFS have already been utilized to address MCDM problems in the areas of cyber security, the internet of things, and Quantum Communication evaluation [48–51]. To far, however, no research has provided an MPSoCs of IoT-specific FFS-based MCDM model for TSCAs countermeasure approaches.

2.6. Studies on CRITIC

There are several uses of the CRITIC approach in recent studies. Abas et al. [52] 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. Wang et al. [53] employed the CRITIC technique to provide a trust evaluation method for service composition in cloud manufacturing. Gaur et al. [31] 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. Khargotra et al. [54] 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. Lin et al. [55] established a thorough evaluation strategy to assess and rank the energy sources using statistical data and the CRITIC technique to weigh qualities. Mishra et al. [56] used CRITIC to determine the relative importance of the multidimensional values to estimate the architectural heritage value for its management in 2021. In addition, Singh [57] 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. Lai et al. [58] 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 to weight TSCA-CTs DM criteria.

2.7. Studies on FDOSM

The FDOSM is a novel MCDM method for ranking the alternatives. FDOSM was proposed recently by Mahmood (2020), 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 (2022) using an Interval-Valued Pythagorean Fuzzy Set with FDOSM as IVP-FDOSM with an assistance of a panel of three experts [35]. In particular, an increasing number of articles deal with applications of FDOSM for efficient (COVID-19) vaccine distribution and related aspects. Among others, [40,41,59] 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. (2021) proposed a model using 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 [37]. 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. (2022) developed a benchmarking model for smart electronic-tourism applications using FDOSM with fuzzy weighted with zero inconsistency method and supported the opinion of eleven expert panels [36].

2.8. Studies on Fermatean fuzzy sets in decision making

L. A. Zadeh laid the basis of the Fuzzy Set (FS) theory in)1965) [14]. 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 [60]. However, increasing MCDM approaches and methods have introduced what are called Fermatean Fuzzy Sets (FFSs) [61] that can manage uncertain information more readily throughout the decision-making to assess the TSCA-CTs in the current study. Table 1 lists more recent contributions in terms of FFSs.

FFSs have five general definitions [42], as in below:

Def 1:

The non-empty set $\boldsymbol{X}$ is defined as the intuitionistic fuzzy sets with objects in the form of:

$$A = \{\langle x, \alpha_A(x), \beta_A(x) \rangle : x \in X\} \tag{1}$$

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

Def 2:

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

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

$$\bar{\boldsymbol{A}} \otimes \bar{\boldsymbol{\beta}} = \boldsymbol{w}_* \left(\boldsymbol{\alpha_A \alpha_B}, \sqrt[3]{\boldsymbol{\beta}_{\mathbf{F}_1}^3 + \boldsymbol{\beta}_{\mathbf{F}_2}^3 - \boldsymbol{\beta}_{\mathbf{F}_1}^3 \boldsymbol{\beta}_{\mathbf{F}_2}^3} \right) \tag{3}$$

$$\partial . \bar{A} = w_* \left(\sqrt[3]{1 - (1 - \alpha_F^3)^{\partial}}, \beta_F^{\partial} \right) \tag{4}$$

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

Where $(\boldsymbol{w})$ is a criterion weight resulted by applying CRITIC.

Def 3:

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

$$\boldsymbol{S}(\bar{\boldsymbol{A}}) = \boldsymbol{\alpha}_{\boldsymbol{A}}^3 + \boldsymbol{\beta}_{\boldsymbol{B}}^3 \tag{6}$$

$$\boldsymbol{T}(\bar{\boldsymbol{A}}) = \boldsymbol{\alpha}_{\boldsymbol{A}}^3 + \boldsymbol{\beta}_{\boldsymbol{B}}^3 \tag{7}$$

The above Eqs. (6) and (7) can be used to compare two FFs, $\bar{\mathbf{A}} = (\alpha_{\mathbf{A}}, \beta_{\mathbf{A}})$ and $\bar{\beta} = (\alpha_{\mathbf{B}}, \beta_{\mathbf{B}})$. In order to compare these two FFs there are three different conditions as listed below:

1) If $\mathbf{S}(\tilde{\mathbf{A}}) < \mathbf{S}(\tilde{\bar{\beta}})$, then $\tilde{\mathbf{A}} < \tilde{\bar{\beta}}$;
2) If $\mathbf{S}(\tilde{\mathbf{A}}) > \mathbf{S}(\bar{\beta})$, then $\tilde{\mathbf{A}} > \tilde{\bar{\beta}}$;
3) If $\mathbf{S}(\tilde{\mathbf{A}}) = \mathbf{S}(\tilde{\bar{\beta}})$
4) then

- $\mathbf{T}(\tilde{\mathbf{A}}) < \mathbf{T}(\tilde{\bar{\beta}})$ then $\tilde{\mathbf{A}} < \tilde{\bar{\beta}}$;
- $\mathbf{T}(\tilde{\mathbf{A}}) > \mathbf{T}(\tilde{\bar{\beta}})$ then $\tilde{\mathbf{A}} > \bar{\beta}$;
- $\mathbf{T}(\tilde{\mathbf{A}}) = \mathbf{T}(\tilde{\bar{\beta}})$ then $\tilde{\mathbf{A}} = \tilde{\bar{\beta}}$.

Def 4:

Table 1
Typical recent studies in terms of FFSs.

Article - Year	Main research contents
[62]-2019	Developed a Fermatean fuzzy WPM decision algorithm to choose the best type of bridge to build.
[63]-2020	In order to expand the flexibility of information aggregation, TOPSIS was extended to Fermatean fuzzy sets based on numerous novel Dombi operators.
[64]-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.
[65]-2022	By combining the Fermatean Fuzzy method with the extensions of SAW, ARAS, and VIKOR, a suitable COVID-19 testing facility was identified.
[66]-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.
[67]-2021	Proposed the CRITIC-COPRAS Fermatean fuzzy approach to deal with the problems of long-term digital transformation.
[68–71] 2013, 2014, 2021	Produced the TODIM and TOPSIS algorithms with the suitable Fermatean fuzzy linguistic set utilizing novel distance measures based on linguistic scale functions.
[72–74] -2022, 2023	Proposed a model to prioritise the COVID-19 patients for Mesenchymal stem cell transfusion, COVID-19 Machine Learning methods, and evaluation defense approaches against MPSoC DoS attack using Fermatean-FDOSM with fuzzy weighted with zero inconsistency for criteria weighting and ranking.

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

$$\boldsymbol{Com}(\tilde{\boldsymbol{A}}) = (\boldsymbol{\beta_A}, \boldsymbol{\alpha_A}) \tag{8}$$

Def 5:

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

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

3. Methodology

This section contains a comprehensive overview of the suggested methodology. The aim of this methodology is to achieve an MPSoCs-based IoT TSCA-CTs evaluation framework depending on the utilized CRITIC and Fermatean-FDOSM methods. The first phase of this methodology is detailed in Sec. 3.1, which describes the TSCA-CTs decision matrix construction and definition process. Afterward, Sec. 3.2 shows the CRITIC objective weighting method of the TSCA-CTs decision matrix phase. Finally, Sec. 3.3 presents the ranking process that resulted in Phase 1 using the Fermatean-FDOSM method. The evaluation framework of TSCA-CTs using CRITIC and Fermatean-FDOSM is illustrated in Fig. 5.

3.1. Phase 1: Decision matrix definition

This phase describes the decision matrix (DM) utilized in evaluating the MPSoCs-based IoT TSCA-CTs. The evaluation of each TSCA-CT is achieved by three primary assessment criteria and their respective ten sub-criteria. The obtained DM is based on the weighted criteria as in Table 2 and evaluated alternatives, as listed in Table 3, of the proposed countermeasure techniques against TSCAs. The word 'criteria' refers to the many metrics that may be used to assess and compare alternatives (e.g., performance and overhead).

3.2. Phase 2: Criteria weighting

Phase 2 presents the TSCA-CTs decision matrix (DM) criteria weighting process using CRITIC technique as displayed in Fig. 5 In order to weight the DM criteria that mentioned in Table 4, there are six stages of the CRITIC technique should be applying [75] as in below:

Stage 1: The DM definition.

This stage includes the defined DM in Phases 1 based on the set of m eligible TSCA-CTs and (n) assessment criteria (i.e., performance). The output of both alternatives and criteria given by $\mathbf{DM}[\mathbf{d_{ij}}]$, with both $\mathbf{i_{th}andj_{th}}$ respectively. See Eq. (10).

$$\mathbf{DM} = [\mathbf{d_{ij}}]_{\mathbf{m\times n}} = \begin{bmatrix} \mathbf{d}_{11} & \mathbf{d}_{12} & \cdots & \mathbf{d}_{1\mathbf{m}} \\ \mathbf{d}_{21} & \mathbf{d}_{22} & \cdots & \mathbf{d}_{2\mathbf{m}} \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{d}_{\mathbf{n}1} & \mathbf{d}_{\mathbf{n}2} & \cdots & \mathbf{d}_{\mathbf{nm}} \end{bmatrix},$$

$$(\boldsymbol{i} = 1, 2, \cdots\cdots \boldsymbol{m};\ \text{and}\ \boldsymbol{j} = 1, 2, \cdots .\boldsymbol{n}) \tag{10}$$

Stage 2: DM normalization.

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

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

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

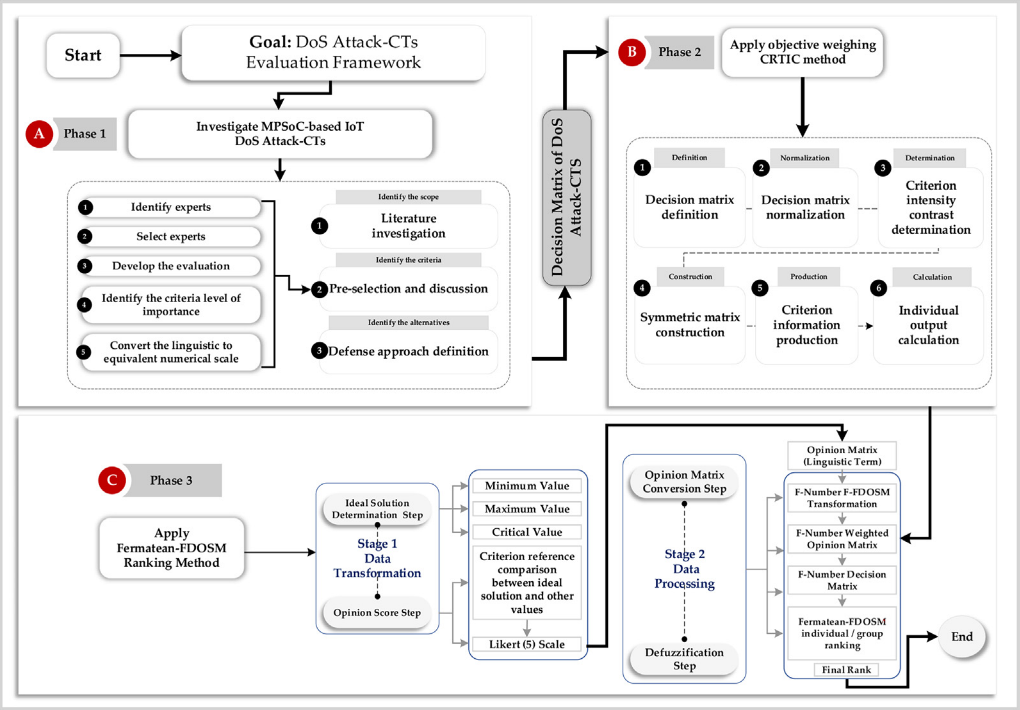

Start
Goal: DoS Attack-CTs Evaluation Framework
A
Phase 1
Investigate MPSoC-based IoT DoS Attack-CTs
1 Identify experts
2 Select experts
3 Develop the evaluation
4 Identify the criteria level of importance
5 Convert the linguistic to equivalent numerical scale
Identify the scope
1 Literature investigation
Identify the criteria
2 Pre-selection and discussion
Identify the alternatives
3 Defense approach definition
Decision Matrix of DoS Attack-CTS
B
Phase 2
Apply objective weighing CRTIC method
Definition
1 Decision matrix definition
Normalization
2 Decision matrix normalization
Determination
3 Criterion intensity contrast determination
Construction
4 Symmetric matrix construction
Production
5 Criterion information production
Calculation
6 Individual output calculation
C
Phase 3
Apply Fermatean-FDOSM Ranking Method
Ideal Solution Determination Step
Stage 1 Data Transformation
Opinion Score Step
Minimum Value
Maximum Value
Critical Value
Criterion reference comparison between ideal solution and other values
Likert (5) Scale
Opinion Matrix Conversion Step
Stage 2 Data Processing
Defuzzification Step
Opinion Matrix (Linguistic Term)
F-Number F-FDOSM Transformation
F-Number Weighted Opinion Matrix
F-Number Decision Matrix
Fermatean-FDOSM individual / group ranking
Final Rank
End

Fig. 5. Methodology phases.

Table 2
DM criteria and sub-criteria explanation.

Criteria	Sub-Criteria	Description	Article
Criteria of Architecture	Number of Routers	Identify the number of routers per NoC architecture involved in the attack scenario.	[9,10,21,24]
	Number of IP Cores	Identify the number of normal IP cores per MPSoC platform involved in the attack scenario.	
	Number of Malicious IP Cores	Identify the number of malicious IP cores per MPSoC platform involved in the attack scenario.	
Criteria of Performance	Throughput	Identify the throughput of IP cores per NoC under different packet injection rates in (flit/cycle) after implementing the countermeasures technique.	
	Bandwidth	Identify the NoC channel bandwidth after implementing the countermeasures technique.	
	Latency	NoC communication latency by (clock/cycle) under different traffic patterns after implementing the countermeasures technique.	
	Power	Identify the power consumption rate by (mW) after implementing the countermeasures technique.	
	Area	Identify the area by (µm2) required for implementing the countermeasures technique.	
Criteria of Overhead	Power (%)	Identify the power overhead after implementing the countermeasures technique.	
	Area (%)	Identify the area overhead after implementing the countermeasures technique.	

Table 3
DM alternatives explanation.

Alternative	Description	Article
Separate Hybrid Router Combined with Separate interface Hybrid Router Combined Hybrid Router	A Countermeasure technique proposed to protect hybrid NoC-based MPSoC routers from TSCAs based on a traffic partitioning defense approach.	[9]
Secure Enhanced Router	A Countermeasure technique uses the communication and security characteristics of the traffic to dynamically configure the router's memory area against TSCAs.	[21]
Random Arbitration Adaptive Routing	A Countermeasure technique based on assigning NoC resources dynamically. They secure the system by isolating communication performance.	[24]
Gossip Router	A Countermeasure technique based on traffic monitor and sending a gossip notification when a threat is detected.	[10]

Table 4
DM used in evaluating TSCA-CTs.

Technique	Architecture			Performance					Overhead	
	No of Routers	No of IPs	No of MIPs	Throughput (Bit/Sec)	Bandwidth	Latency (clock/cycle)	Area (µm^2)	Power (mW)	Area %	Power %
Separate Hybrid	16	16	1	0.8	0.2	7	53,104	7.82	0.07	0.33
Combined with Separate interface Hybrid	16	16	1	0.5	0.2	8	55160.32	8.1	0.11	0.34
Combined Hybrid	16	16	1	1	0.2	7	59055.04	7.12	0.19	0.32
Secure Enhanced Router	9	9	1	0.6	0.9	3.2	1543.93	2.5	0.09	0.08
Random Arbitration	16	16	1	0.42	1	1.3	169.83	2.4	0.11	0.09
Adaptive Routing	16	16	1	0.51	1	1.4	77.19	2.3	0.05	0.08
Gossip Router	16	16	3	2.23	0.1	7	3189	2.4	0.21	0.16

Stage 3: Contrast intensity determination.

The intensity of the contrast can be determined using the standard deviation of normalized criterion values in the columns $\boldsymbol{d_j}$. The estimation of the standard deviation of each criterion can be obtained by using Eq. (12).

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

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

Stage 4: Symmetric matrix construction.

In this stage, a symmetric matrix ($\boldsymbol{m} \times \boldsymbol{n}$) will build involving a term $\boldsymbol{r_{jk}}$ to express correlation coefficients such as the criteria's correlation coefficient as in Eq. (13).

$$r_{jk} = \frac{\Sigma_{i=1}^{m}\left(\bar{d}_{ij} - \bar{d}_j\right)\Sigma_{i=1}^{m}\left(\bar{d}_{ij} - \bar{d}_j\right)\left(\bar{d}_{ik} - \bar{d}_k\right)}{\sqrt{\Sigma_{i=1}^{m}\left(\bar{d}_{ij} - \bar{d}_j\right)^2 \Sigma_{i=1}^{m}\left(\bar{d}_{jk} - \bar{d}_k\right)^2}} \tag{13}$$

Stage 5: Criterion information production.

This stage depicts the results of Eqs. (12) and (13) for specifying the criterion information ($\boldsymbol{C_j}$) as in Eq. (14).

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

Stage 6: Weight calculation.

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

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

The criteria weighting results will feed to the next Phase 3 alternatives ranking in order to extract the final rank of each alternative (countermeasure technique) per DM shown in Table 4.

3.3. Phase 3: Alternatives ranking

This phase explains the stages of Fermatean-FDOSM [34,41,61] used in TSCA-CTs DM ranking, as shown in methodology phases

(Fig. 5). We can summarize the procedure of Fermatean-FDOSM ranking method in three stages as in below:

Stage 1: Data input.

The data input stage is the DM that is built from the intersection of TSCA-CTs criteria, and alternatives see Sec. 3.1 to get the TSCA-CTs DM formatted based on $(\boldsymbol{m} \times \boldsymbol{n})$ sets of $(\boldsymbol{A}_1, \ \boldsymbol{A}_2 \ldots\ldots \ \boldsymbol{A}_{\boldsymbol{m}})$ alternatives and $(\boldsymbol{C}_1, \boldsymbol{C}_2 \ldots\ldots \boldsymbol{C}_{\boldsymbol{n}})$ of criteria respectively as shown in below:

$$\boldsymbol{DM} = \begin{array}{c} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \\ \vdots \\ \boldsymbol{A}_m \end{array} \begin{bmatrix} \boldsymbol{x}_{11} & \boldsymbol{x}_{12} & \cdots & \boldsymbol{x}_{1n} \\ \boldsymbol{x}_{21} & \boldsymbol{x}_{22} & \cdots & \boldsymbol{x}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{x}_{m1} & \boldsymbol{x}_{m2} & \cdots & \boldsymbol{x}_{mn} \end{bmatrix}$$

Stage 2: Data transformation.

This stage includes the following steps:

(i) Utilize Eq. (16) to choose the ideal (optimal) solution from a set of criteria presented in a (Min, Max, and Critical) range.

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

Fundamentally, (**max**) refers to the ideal value with the benefit of criteria, (**min**) refers to the ideal solution, the criteria cost, finally ($\mathbf{Op_{ij}}$) is the critical value, while the best value (optimal solution) falls within (**max**) and (**min**).

(ii) Identify a team of subject-matter experts (someone who knows a lot about the topic at hand and has worked in the field for a while). To distinguish them from "normative experts," who specialize in statistics and subjective probability, the literature sometimes refers to these individuals as "domain" or "substantive" experts. In this study, we used bibliometric analysis of all cited authors and co-authors to determine which researchers were most knowledgeable about MPSoCs-based IoT security issues and so should be selected as experts. There are three professionals contributing to this study.

(iii) 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.

(iv) Transform the expert's opinion matrix to the equivalent numerical matrix using the linguistic Likert scale. The Likert scale suggests that the TSCA-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 Table 5 and Eq. (17).

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

where $\otimes$ refers to the establishment comparison between ideal solution and alternatives [34].

(v) Adopt the opinion matrix that is based on expert opinion, as shown in Table 7, then get the final output of this stage just as transformed to the fuzzy opinion matrix using Fermatean Fuzzy Set (FFS) as below:

Table 5
A five-point Likert scale, numerical scale, and Fermatean Fuzzy Set (FFS).

Numerical scoring scale	A linguistic scorning scale	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

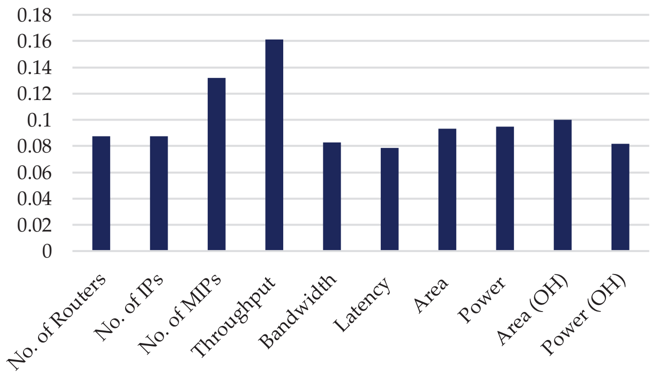


Fig. 6. TSCA-CTs DM criteria weights according to CRITIC method.

$$\mathbf{Op_{Lang}} = \begin{array}{c} \mathbf{A}_1 \\ \vdots \\ \mathbf{A_m} \end{array} \begin{bmatrix} \mathbf{Op}_{11} & \cdots & \mathbf{Op_{1n}} \\ \vdots & \ddots & \vdots \\ \mathbf{Op_{m1}} & \cdots & \mathbf{Op_{mn}} \end{bmatrix}$$

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

Stage 3: Data Processing.

(i) This stage represents the final stage for fuzzy decision matrix ranking, as shown in Fig. 6.

(ii) There are two approaches for ranking based on individual and group experts' opinions [34]. 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 Eq. (18).

$$\bar{\boldsymbol{x}} = \frac{1}{\boldsymbol{n}} \Sigma_{\boldsymbol{i}=1}^{\boldsymbol{n}} \boldsymbol{x}_{\boldsymbol{i}} \tag{18}$$

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

(iii) The final rank and score achievement by the defuzzification process for alternatives occurred based on *Def 3* and *Def 5* as well as by using Eq. (6) and Eq. (9), where the best alternative is associated with a high score.

4. Discussion results

This section exhibits the evaluation and classification results of TSCA-CTs to improve security in the context of MPSoCs-based IoT platforms. This section is separated into three 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 TSCA-CTs DM alternatives based on individual and group decision-making Fermatean-FDOSM are then presented. Finally, the section "Discussion Results" and "Validation ranking results" section in order to validates the final results of the ranking process.

4.1. The criteria weighting results

This section shows the criteria weights of TSCA-CTs of DM using the CRTIC method as developed in Sec. 3.2. As we mentioned, the CRITIC approach has six stages to be applied to compute the DM criteria weights. The obtained weights after applying Eq. (11) to

Table 6
CRITIC DM weighting results.

Criteria	Wright
No. of Routers	0.0877
No. of IPs	0.0877
No. of MIPs	0.1319
Throughput	0.1614
Bandwidth	0.0827
Latency	0.07863
Area	0.0933
Power	0.0947
Area (OH)	0.1
Power (OH)	0.08164

*Area and Power Over Head (OH) are the costs due to implementing the countermeasure technique.

normalize the DM into the interval of (0 to 1) and then using Eq. (12) to determine the intensity of the contrast using the standard deviation of normalized criterion values. Moreover, Eq. (13) was utilized after obtaining a symmetric matrix to express the criteria's correlation coefficient. Furthermore, Eq. (14) and Eq. (15) were used for criterion information production and weight calculation for every ten criteria, respectively. Both Table 6 and Fig. 6 display the weight results, which indicate the vital (significant) variation of ten criteria of TSCA-CTs based on the CRITIC technique. The NoC throughput received the highest weight as the first vital criterion, followed by the number of malicious IP cores (No. of MIPs) utilized by adversaries to implement the attacks on MPSoCs-based IoT platforms as a second vital criterion.

Consequently, the NoC latency received the lowest weight as the sixth important criterion. Besides, the NoC number of routers and number of normal IP cores have received the same importance as the first and second lowest importance criteria. In addition, the NoC bandwidth and power overhead have received the same importance as the fifth and last criteria. Finally, the NoC consumption power and utilized area have received the third and fourth 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 submitted to Fermatean-FDOSM to calculate the final rank of seven TSCA-CTs.

4.2. The alternatives ranking results

The results and discussion in this section relate to evaluating the TSCA-CTs based on Fermatean-FDOSM individual and group of experts' opinions. Each expert records their opinion using DM in Table 7 with the purpose of identifying the optimal solution for each criterion, then applies Eq. (16) and Eq. (17) to compare the optimal solution with other values per criterion/alternative using linguist terms. By using the Likert five scale approach, the three experts presented the opinion matrix as illustrated in Table 7.

The resulting three experts' opinion matrices will be converted to a fuzzy opinion matrix using the Fermatean fuzzy set (FFS) by applying Eq. (2), as shown in Table 11.

In order to aggregate the FFS values of each alternative, there are two approaches, as mentioned in Phase 2. The criteria weighting results will feed to the next Phase 3 alternatives ranking in order to extract the final rank of each alternative (countermeasure technique) per DM as shown in Fig. 7.

(i) Individual decision-making can be calculated using Eq. (3) and Eq. (4); the results are shown in Table 8. From expert 1 point of view (Separate Hybrid) is the most powerful countermeasure technique, while expert 2 appointed (Combined Hybrid) as the best defence approach, in contrast to expert 3 selected the (Gossip Router); based on the above, there is a wide range of options for determining the most effective method of countermeasure against TSCA linked with the

Table 7
Opinion matrix of three experts.

Expert 1: Opinion Matrix										
Technique	Architecture			Performance				Overhead		
	No of Routers	No of IPs	No of MIPs	Throughput	Bandwidth	Latency	Area	Power	Area%	Power%
Separate Hybrid	ND	ND	D	ND	D	BD	BD	ND	D	D
Combined with Separate interface Hybrid	ND	ND	D	SD	D	BD	BD	SD	D	D
Combined Hybrid	ND	ND	D	SD	D	BD	BD	SD	ND	SD
Secure Enhanced Router	ND	ND	D	SD	ND	D	ND	D	D	ND
Random Arbitration	ND	ND	D	D	SD	ND	D	D	BD	SD
Adaptive Routing	ND	ND	D	D	SD	SD	BD	D	SD	ND
Gossip Router	ND	ND	ND	HD	BD	BD	BD	D	BD	HD
Expert 2: Opinion Matrix										
Separate Hybrid	ND	ND	ND	BD	BD	D	HD	BD	BD	BD
Combined with Separate interface Hybrid	ND	ND	ND	HD	BD	ND	HD	HD	BD	BD
Combined Hybrid	ND	ND	ND	ND	BD	D	HD	BD	HD	BD
Secure Enhanced Router	ND	ND	ND	BD	D	BD	HD	SD	DB	SD
Random Arbitration	ND	ND	ND	BD	ND	HD	BD	SD	BD	ND
Adaptive Routing	ND	ND	ND	BD	ND	HD	ND	ND	ND	SD
Gossip Router	ND	ND	BD	HD	HD	D	HD	SD	HD	BD
Expert 3: Opinion Matrix										
Separate Hybrid	ND	ND	HD	BD	HD	ND	HD	BD	SD	D
Combined with Separate interface Hybrid	ND	ND	HD	HB	HD	SD	HD	BD	D	D
Combined Hybrid	ND	ND	HD	BD	HD	ND	HD	D	HD	D
Secure Enhanced Router	ND	ND	HD	D	SD	HD	HD	SD	D	ND
Random Arbitration	ND	ND	HD	D	ND	BD	D	SD	D	SD
Adaptive Routing	ND	ND	HD	D	ND	BD	ND	ND	ND	SD
Gossip Router	ND	ND	ND	ND	HD	ND	HD	SD	HD	BD

*The linguistic five levels scale of importance, NoDifference (ND), SlightDifference (SD), Difference (D), BigDifference (BD), and HugeDifference (HD). See Table 5.

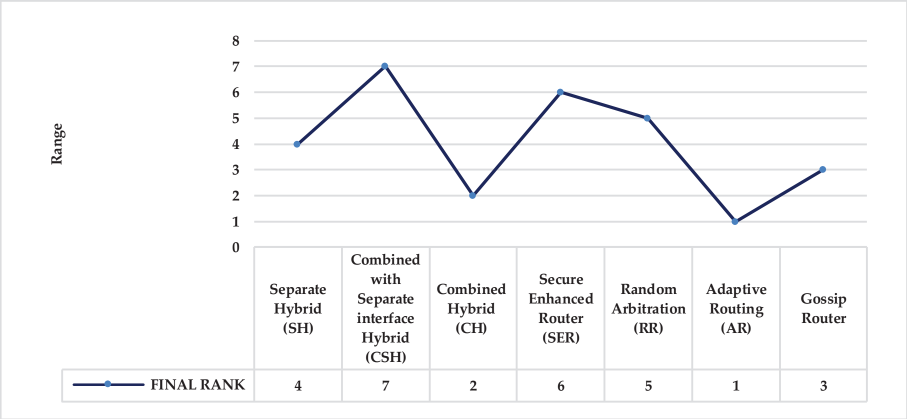


Fig. 7. The graph of group decision-making evaluation.

Table 8
TSCA-CTs evaluation results based on individual decision-making F-DOSM.

Techniques	Expert 1		Expert 2		Expert 3	
	score	rank	score	rank	score	rank
Separate Hybrid	0.005278836	1	0.003027946	5	0.002049521	4
Combined with Separate interface Hybrid	0.003725028	4	0.003109792	4	0.001426353	7
Combined Hybrid	0.00449195	2	0.005874342	1	0.001697463	6
Secure Enhanced Router	0.004327566	3	0.002747787	6	0.002017986	5
Random Arbitration	0.002870893	7	0.004085557	3	0.002760703	3
Adaptive Routing	0.003201689	5	0.005425538	2	0.004118656	2
Gossip Router	0.002892799	6	0.001531223	7	0.006466303	1

individual decision-making approach. There is a continuing need for a group decision-making method to get the final rank.

(ii) Group decision-making can be calculated using Eq. (18); the results are shown in Table 9. However, Fig. 7 illustrates the final graph of group decision-making evaluation results, indicating that the Adaptive Routing countermeasure technique has the first evaluation score. In contrast, the Combined with Separate interface Hybrid countermeasure technique has the last evaluation score.

4.3. Validation ranking results

This section provides the validation of group decision-making evaluation results discussed in previous Sec. 4.2 According to [34,76,77], the procedure of evaluation results validation has been followed. To justify the group decision-making evaluation results of TSCA-CTs, the validation process was implemented by dividing the countermeasure techniques into two groups and then aggregating all opinion matrices to produce a unified opinion matrix.

Table 9
TSCA-CTs evaluation results based on group decision-making F-DOSM.

Technique	Final score	Final rank
Separate Hybrid	0.003452101	4
Combined with Separate interface Hybrid	0.002753724	7
Combined Hybrid	0.004021251	2
Secure Enhanced Router	0.003031113	6
Random Arbitration	0.003239051	5
Adaptive Routing	0.004248628	1
Gossip Router	0.003630108	3

The countermeasure techniques are ordered in the decision matrix according to the group decision-making approach. The arithmetic mean ($\bar{x}$) of each group is computed using below Eq. (19), as we discussed in Phase 3.

$$\bar{x} = \frac{1}{n}\Sigma_{i=1}^{n} x_i \tag{19}$$

The comparison was based on the mean of the results from each group. Because the expert (decision makers) assigned the lowest linguistic concepts to the ideal solution of each criterion, the lowest mean values of each group produced legitimate findings, which is the FDOSM method's basic concept. As a consequence, the first group is assumed to have the lowest mean in order to test the validity of the result; it is then compared to the second group, confirming the result validity, as seen in Table 10. The statistical validation findings of the groups' TSCA-CTs are acceptable and have been systematically evaluated (ranked).

Table 10
Validation of group TSCA-CTs results.

Groups	Alternatives	Mean
1st group	Adaptive Routing Random Arbitration Secure Enhanced Router	2.363636
2nd group	Combined Hybrid Gossip Router Separate Hybrid Combined with Separate interface Hybrid	2.901515

Table 11
Fuzzy opinion matrix of three experts.

Expert 1: Fuzzy Opinion Matrix																				
Technique	**No of Routers**		**No of IPs**		**No of MIPs**															
Throughput																				
Bandwidth		**Latency**		**Area (µm2)**		**Power**		**Area%**		**Power%**										
Separate Hybrid	0.9	0.1	0.9	0.1	0.5	0.45	0.9	0.1	0.5	0.45	0.35	0.6	0.35	0.6	0.9	0.1	0.5	0.45	0.5	0.45
Combined with Separate interface Hybrid	0.9	0.1	0.9	0.1	0.5	0.45	0.75	0.2	0.5	0.45	0.35	0.6	0.35	0.6	0.75	0.2	0.5	0.45	0.5	0.45
Combined Hybrid	0.9	0.1	0.9	0.1	0.5	0.45	0.75	0.2	0.5	0.45	0.35	0.6	0.35	0.6	0.75	0.2	0.9	0.1	0.75	0.2
Secure Enhanced Router	0.9	0.1	0.9	0.1	0.5	0.45	0.75	0.2	0.9	0.1	0.5	0.45	0.9	0.1	0.5	0.45	0.5	0.45	0.9	0.1
Random Arbitration	0.9	0.1	0.9	0.1	0.5	0.45	0.5	0.45	0.75	0.2	0.9	0.1	0.5	0.45	0.5	0.45	0.35	0.6	0.75	0.2
Adaptive Routing	0.9	0.1	0.9	0.1	0.5	0.45	0.5	0.45	0.75	0.2	0.75	0.2	0.35	0.6	0.5	0.45	0.75	0.2	0.9	0.1
Gossip Router	0.9	0.1	0.9	0.1	0.9	0.1	0.1	0.9	0.35	0.6	0.35	0.6	0.35	0.6	0.5	0.45	0.35	0.6	0.1	0.9
Expert 2: Fuzzy Opinion Matrix																				
Separate Hybrid	0.9	0.1	0.9	0.1	0.9	0.1	0.35	0.6	0.35	0.6	0.5	0.45	0.1	0.9	0.35	0.6	0.35	0.6	0.35	0.6
Combined with Separate interface Hybrid	0.9	0.1	0.9	0.1	0.9	0.1	0.1	0.9	0.35	0.6	0.9	0.1	0.1	0.9	0.1	0.9	0.35	0.6	0.35	0.6
Combined Hybrid	0.9	0.1	0.9	0.1	0.9	0.1	0.9	0.1	0.35	0.6	0.5	0.45	0.1	0.9	0.35	0.6	0.1	0.9	0.35	0.6
Secure Enhanced Router	0.9	0.1	0.9	0.1	0.9	0.1	0.35	0.6	0.5	0.45	0.35	0.6	0.1	0.9	0.75	0.2	0.35	0.6	0.75	0.2
Random Arbitration	0.9	0.1	0.9	0.1	0.9	0.1	0.35	0.6	0.9	0.1	0.1	0.9	0.35	0.6	0.75	0.2	0.35	0.6	0.9	0.1
Adaptive Routing	0.9	0.1	0.9	0.1	0.9	0.1	0.35	0.6	0.9	0.1	0.1	0.9	0.9	0.1	0.9	0.1	0.9	0.1	0.75	0.2
Gossip Router	0.9	0.1	0.9	0.1	0.35	0.6	0.1	0.9	0.1	0.9	0.5	0.45	0.1	0.9	0.75	0.2	0.1	0.9	0.35	0.6
Expert 3: Fuzzy Opinion Matrix																				
Separate Hybrid	0.9	0.1	0.9	0.1	0.1	0.9	0.35	0.6	0.1	0.9	0.9	0.1	0.1	0.9	0.35	0.6	0.75	0.2	0.5	0.45
Combined with Separate interface Hybrid	0.9	0.1	0.9	0.1	0.1	0.9	0.1	0.9	0.1	0.9	0.75	0.2	0.1	0.9	0.35	0.6	0.5	0.45	0.5	0.45
Combined Hybrid	0.9	0.1	0.9	0.1	0.1	0.9	0.35	0.6	0.1	0.9	0.9	0.1	0.1	0.9	0.5	0.45	0.1	0.9	0.5	0.45
Secure Enhanced Router	0.9	0.1	0.9	0.1	0.1	0.9	0.5	0.45	0.75	0.2	0.1	0.9	0.1	0.9	0.75	0.2	0.5	0.45	0.9	0.1
Random Arbitration	0.9	0.1	0.9	0.1	0.1	0.9	0.5	0.45	0.9	0.1	0.35	0.6	0.5	0.45	0.75	0.2	0.5	0.45	0.75	0.2
Adaptive Routing	0.9	0.1	0.9	0.1	0.1	0.9	0.5	0.45	0.9	0.1	0.35	0.6	0.9	0.1	0.9	0.1	0.9	0.1	0.75	0.2
Gossip Router	0.9	0.1	0.9	0.1	0.9	0.1	0.9	0.1	0.1	0.9	0.9	0.1	0.1	0.9	0.75	0.2	0.1	0.9	0.35	0.6
Secure Enhanced Router	0.9	0.1	0.9	0.1	0.1	0.9	0.5	0.45	0.75	0.2	0.1	0.9	0.1	0.9	0.75	0.2	0.5	0.45	0.9	0.1
Random Arbitration	0.9	0.1	0.9	0.1	0.1	0.9	0.5	0.45	0.9	0.1	0.35	0.6	0.5	0.45	0.75	0.2	0.5	0.45	0.75	0.2
Adaptive Routing	0.9	0.1	0.9	0.1	0.1	0.9	0.5	0.45	0.9	0.1	0.35	0.6	0.9	0.1	0.9	0.1	0.9	0.1	0.75	0.2
Gossip Router	0.9	0.1	0.9	0.1	0.9	0.1	0.9	0.1	0.1	0.9	0.9	0.1	0.1	0.9	0.75	0.2	0.1	0.9	0.35	0.6

5. Conclusion

Using the new MCDM technique known as Fermatean-FDOSM, the TSCA-CTs were evaluated in terms of MPSoCs-based IoT. This research was conducted in three phases, which are shown in Fig. 5. The first phase is to create a DM for TSCAs and CTs. The CRITIC approach, comprised of six stages, is used in the second phase to weight DM criteria, while the Fermatean-FDOSM method, comprised of three stages , is used in the third phase to rank DM alternatives. The key takeaway from this research is an assessment methodology for choosing the best effective countermeasure strategy against TSCAs in terms of MPSoCs-based IoT. The arithmetic mean method is used to verify the accuracy of the evaluation findings.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Fernandes R, Marcon C, Cataldo R, Sepulveda J. Using smart routing for secure and dependable NoC-Based MPSoCs. IEEE/ACM Trans Netw 2020;28 (3):1158–71. doi: https://doi.org/10.1109/TNET.2020.2979372.

[2] Indrusiak LS, Harbin J, Reinbrecht C, Sepúlveda J. Side-channel protected MPSoC through secure real-time networks-on-chip. Microprocess Microsyst 2019;68:34–46. doi: https://doi.org/10.1016/j.micpro.2019.04.004.

[3] Sant'Ana AC, Medina H, Moraes FG. Security vulnerabilities and countermeasures in MPSoCs. IEEE Des TEST 2021;38(4):70–7. doi: https://doi.org/10.1109/MDAT.2021.3049710.

[4] Sharma G, Bousdras G, Ellinidou S, Markowitch O, Dricot JM, Milojevic D. Exploring the security landscape: NoC-based MPSoC to Cloud-of-Chips. Microprocess Microsyst 2021;84:. doi: https://doi.org/10.1016/j.micpro.2021.103963103963.

[5] Saponara S, Fanucci L. Homogeneous and heterogeneous MPSoC architectures with network-on-chip connectivity for low-power and real-time multimedia signal processing. VLSI Des 2012;2012:1–17. doi: https://doi.org/10.1155/2012/450302.

[6] Bhunia S, Hsiao MS, Banga M, Narasimhan S. Hardware trojan attacks: Threat analysis and countermeasures. Proc IEEE 2014;102(8):1229–47. doi: https://doi.org/10.1109/JPROC.2014.2334493.

[7] Lv YQ, Zhou Q, Cai YC, Qu G. Trusted integrated circuits: The problem and challenges. J Comput Sci Technol 2014;29(5):918–28. doi: https://doi.org/10.1007/s11390-014-1479-9.

[8] Reinbrecht C, Forlin B, Sepúlveda J. Cache timing attacks on NoC-based MPSoCs. Microprocess Microsyst 2019;66:1–9. doi: https://doi.org/10.1016/j.micpro.2019.01.007.

[9] Biswas AK. Efficient timing channel protection for hybrid (packet/circuit-switched) network-on-chip. IEEE Trans Parallel Distrib Syst 2018;29 (5):1044–57. doi: https://doi.org/10.1109/TPDS.2017.2783337.

[10] Reinbrecht C, Susin A, Bossuet L, Sepúlveda J, Gossip NoC - Avoiding timing side-channel attacks through traffic management. In: *Proc IEEE Comput Soc Annu Symp VLSI, ISVLSI*, vol. 2016-Septe, pp. 601–606, 2016, doi: 10.1109/ISVLSI.2016.25.

[11] Reinbrecht C, Aljuffri A, Hamdioui S, Taouil M, Forlin B, Sepulveda J, Guard-NoC: A protection against side-channel attacks for MPSoCs. In: *Proc IEEE Comput Soc Annu Symp VLSI, ISVLSI*, vol. 2020-July, pp. 536–541, 2020, doi: 10.1109/ISVLSI49217.2020.000-1.

[12] Ali U, Khan O, ConNOC: A practical timing channel attack on network-on-chip hardware in a multicore processor, pp. 192–202, 2022, doi: 10.1109/host49136.2021.9702280.

[13] Biswas AK, Sikdar B. Protecting network-on-chip intellectual property using timing channel fingerprinting. ACM Trans Embed Comput Syst 2022;21 (2):1–21. doi: https://doi.org/10.1145/3495565.

[14] Zadeh LA. Fuzzy sets. Inf Control 1965;8(3):338–53. doi: https://doi.org/10.1016/S0019-9958(65)90241-X.

[15] Sharma G, Bousdras G, Ellinidou S, Markowitch O, Dricot JM, Milojevic D. Exploring the security landscape: NoC-based MPSoC to Cloud-of-Chips. Microprocess Microsyst 2019;84(November):2021. doi: https://doi.org/10.1016/j.micpro.2021.103963.

[16] Charles S, Mishra P. A survey of network-on-chip security attacks and countermeasures. ACM Comput Surv 2021;54(5):pp. doi: https://doi.org/10.1145/3450964.

[17] Carreon NA, Lu S, Lysecky R. Probabilistic estimation of threat intrusion in embedded systems for runtime detection. ACM Trans Embed Comput Syst 2021;20(2):pp. doi: https://doi.org/10.1145/3432590.

[18] Sepúlveda J, Gogniat G, Flórez D, Diguet JP, Zeferino C, Strum M, Elastic security zones for NoC-based 3D-MPSoCs. In: *2014 21st IEEE Int Conf Electron Circuits Syst ICECS 2014*, pp. 506–509, 2014, doi: 10.1109/ICECS.2014.7050033.

[19] Daoud L. Secure network-on-chip architectures for MPSoC: Overview and challenges. Midwest Symp Circuits Syst 2019;2018:542–3. doi: https://doi.org/10.1109/MWSCAS.2018.8623831.

[20] Wang Y, Suh GE, Efficient timing channel protection for on-chip networks. In: *Proc. 012 6th IEEE/ACM Int Symp Networks-on-Chip, NoCS 2012*, pp. 142–151, 2012, doi: 10.1109/NOCS.2012.24.

[21] Sepúlveda J, Flórez D, Soeken M, Diguet JP, Gogniat G, Dynamic NoC buffer allocation for MPSoC timing side channel attack protection. In: *LASCAS 2016 - 7th IEEE Lat. Am. Symp. Circuits Syst. R9 IEEE CASS Flagsh. Conf.*, pp. 91–94, 2016, doi: 10.1109/LASCAS.2016.7451017.

[22] Sepulveda J, Florez D, Fernandes R, Marcon C, Gogniat G, Sigl G, Towards risk aware NoCs for data protection in MPSoCs. In: *2016 11th Int. Symp. Reconfigurable Commun. Syst. ReCoSoC 2016*, 2016, doi: 10.1109/ReCoSoC.2016.7533898.

[23] Reinbrecht C, Susin A, Bossuet L, Sigl G, Sepúlveda J. Timing attack on NoC-based systems: Prime+Probe attack and NoC-based protection. Microprocess Microsyst 2017;52:556–65. doi: https://doi.org/10.1016/j.micpro.2016.12.010.

[24] Sepúlveda MJ, Diguet JP, Strum M, Gogniat G. NoC-based protection for SoC time-driven attacks. IEEE Embed Syst Lett 2015;7(1):7–10. doi: https://doi.org/10.1109/LES.2014.2384744.

[25] Guo S, Wang J, Chen Z, Lu Z, Guo J, Yang L. Security-aware task mapping reducing thermal side channel leakage in CMPs. IEEE Trans Ind Informatics 2019;15(10):5435–43. doi: https://doi.org/10.1109/TII.2019.2904092.

[26] Reinbrecht C, Susin A, Bossuet L, Sigl G, Sepulveda J, Side channel attack on NoC-based MPSoCs are practical: NoC Prime+Probe attack. In: *Proc. - SBCCI 2016 29th Symp. Integr. Circuits Syst. Des. Chip Mt.*, pp. 1–6, 2016, doi: 10.1109/SBCCI.2016.7724051.

[27] Ancajas DM, Chakraborty K, Roy S, Fort-NoCs: Mitigating the threat of a compromised NoC. In: *Proc - Des Autom Conf*, no. Section 4, 2014, doi: 10.1145/2593069.2593144.

[28] Indrusiak LS, Harbin J, Sepulveda MJ, Side-channel attack resilience through route randomisation in secure real-time Networks-on-Chip. In: *12th Int Symp Reconfigurable Commun Syst ReCoSoC 2017 - Proc.*, 2017, doi: 10.1109/ReCoSoC.2017.8016142.

[29] Al-Hchaimi AAJ, Flayyih WN, Hashim F, Rusli MS, Rokhani FZ, Review of 3D networks-on-chip simulators and plugins. In: *2021 IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia)*, 2021, pp. 17–20. doi: 10.1109/PrimeAsia51450.2021.9701472.

[30] Diakoulaki D, Mavrotas G, Papayannakis L. Determining objective weights in multiple criteria problems: The critic method. Comput Oper Res 1995;22(7):763–70. doi: https://doi.org/10.1016/0305-0548(94)00059-H.

[31] Gaur S, Dosapati S, Tawalare A. Stakeholder assessment in construction projects using a CRITIC-TOPSIS approach. Built Environ Proj Asset Manag 2023;13(2):217–37. doi: https://doi.org/10.1108/BEPAM-10-2021-0122.

[32] Silvius G, Schipper R. Planning project stakeholder engagement from a sustainable development perspective. Adm Sci 2019;9(2). doi: https://doi.org/10.3390/admsci9020046.

[33] Stević Ž, Pamučar D, Puška A, Chatterjee P. Sustainable supplier selection in healthcare industries using a new MCDM method: Measurement of alternatives and ranking according to COmpromise solution (MARCOS). Comput Ind Eng 2020;140:. doi: https://doi.org/10.1016/j.cie.2019.106231106231.

[34] Salih MM, Zaidan BB, Zaidan AA. Fuzzy decision by opinion score method. Appl Soft Comput J 2020;96:106595.

[35] Al-Samarraay MS, Salih MM, Ahmed MA, Zaidan AA, Albahri OS, Pamucar D, et al. A new extension of FDOSM based on Pythagorean fuzzy environment for evaluating and benchmarking sign language recognition systems. Neural Comput Appl 2022;34(6):4937–55.

[36] Alamoodi AH, Mohammed RT, Albahri OS, Qahtan S, Zaidan AA, Alsattar HA, et al. Based on neutrosophic fuzzy environment: a new development of FWZIC and FDOSM for benchmarking smart e-tourism applications. Complex Intell Syst 2022;8(4):3479–503.

[37] Mahmoud US, et al., A methodology of DASs benchmarking to support industrial community characteristics in designing and implementing advanced driver assistance systems within vehicles, 2021.

[38] Salih MM, Albahri OS, Zaidan AA, Zaidan BB, Jumaah FM, Albahri AS. Benchmarking of AQM methods of network congestion control based on extension of interval type-2 trapezoidal fuzzy decision by opinion score method. Telecommun Syst 2021;77(3):493–522. doi: https://doi.org/10.1007/s11235-021-00773-2.

[39] Al-Samarraay MS, Zaidan AA, Albahri OS, Pamucar D, AlSattar HA, Alamoodi AH, et al. 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[Formula presented]. Appl Soft Comput 2022;116. doi: https://doi.org/10.1016/j.asoc.2021.108284.

[40] Albahri AS, Albahri OS, Zaidan AA, Alnoor A, Alsattar HA, Mohammed R, et al. 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 Stand Interfaces 2022;80. doi: https://doi.org/10.1016/j.csi.2021.103572.

[41] Alsalem MA, Alsattar HA, Albahri AS, Mohammed RT, Albahri OS, Zaidan AA, et al. Based on T-spherical fuzzy environment: A combination of FWZIC and FDOSM for prioritising COVID-19 vaccine dose recipients. J Infect Public Health 2021;14(10):1513–59.

[42] Senapati T, Yager RR. Fermatean fuzzy sets. J Ambient Intell Humaniz Comput 2020;11(2):663–74. doi: https://doi.org/10.1007/s12652-019-01377-0.

[43] Yager RR. Pythagorean membership grades in multicriteria decision making. IEEE Trans Fuzzy Syst 2014;22(4):958–65. doi: https://doi.org/10.1109/TFUZZ.2013.2278989.

[44] Atanassov KT. Intuitionistic fuzzy sets. Fuzzy Sets Syst 1986;20(1):87–96. doi: https://doi.org/10.1016/S0165-0114(86)80034-3.

[45] J., s,. Ordering of interval-valued Fermatean fuzzy sets and its applications. Expert Syst Appl 2021;185(July). doi: https://doi.org/10.1016/j.eswa.2021.115613.

[46] Shahzadi G, Zafar F, Alghamdi MA, Feng F. Multiple-attribute decision-making using Fermatean fuzzy Hamacher interactive geometric operators. Math Probl Eng 2021;2021:1–20.

[47] Simić V, Ivanović I, Đorić V, Torkayesh AE. Adapting urban transport planning to the COVID-19 pandemic: An integrated Fermatean fuzzy model. Sustain Cities Soc 2022;79(January). doi: https://doi.org/10.1016/j.scs.2022.103669.

[48] Aldring J, Ajay D. MABAC method for assessment of cyber security technologies under Fermatean fuzzy sets. In: Evolution in Computational Intelligence. Springer; 2022. p. 441–50.

[49] Kabak M, Aydın S, Aktaş A, Internet of things Fermatean fuzzy CRITIC testing procedure for new normal. In: *International Conference on Intelligent and Fuzzy Systems*, 2022, pp. 649–655.

[50] . Kamali Saraji M, Streimikiene D, Kyriakopoulos GL, Fermatean fuzzy CRITIC-COPRAS method for evaluating the challenges to industry 4.0 adoption for a sustainable digital transformation, *Sustainability*, 2021; 13(17): 9577.

[51] Cao C, Zhang M. Credit risk evaluation of quantum communications listed companies in China based on Fermatean fuzzy TOPSIS. Procedia Comput Sci 2022;199:361–8.

[52] Abas M, Alkahtani M, Khalid QS, Hussain G, Abidi MH, Buhl J. Parametric study and optimization of end-milling operation of AISI 1522H steel using definitive screening design and multi-criteria decision-making approach. Materials (Basel) 2022;15(12):pp. doi: https://doi.org/10.3390/ma15124086.

[53] Wang F, Laili Y, Zhang L. Trust evaluation for service composition in cloud manufacturing using GRU and association analysis. IEEE Trans Ind Informatics 2023;19(2):1912–22.

[54] Khargotra R, Kumar R, András K, Fekete G, Singh T. Thermo-hydraulic characterization and design optimization of delta-shaped obstacles in solar water heating system using CRITIC-COPRAS approach. Energy 2022;261(August):. doi: https://doi.org/10.1016/j.energy.2022.125236125236.

[55] Lin S-S, Shen S-L, Zhou A. Energy sources evaluation based on multi-criteria decision support approach in China. Sustain Horizons 2022;2(May):. doi: https://doi.org/10.1016/j.horiz.2022.100017100017.

[56] Mishra PS, Muhuri S. Value assessment of existing architectural heritage for future generation using criteria importance through inter-criteria correlation and grey relational analysis method: A case of Odisha temple architecture in India. Curr Sci 2021;121(6):823–33. doi: https://doi.org/10.18520/cs/v121/i6/823-833.

[57] Singh T. Optimum design based on fabricated natural fiber reinforced automotive brake friction composites using hybrid CRITIC-MEW approach. J Mater Res Technol 2021;14:81–92. doi: https://doi.org/10.1016/j.jmrt.2021.06.051.

[58] Lai H, Liao H. A multi-criteria decision making method based on DNMA and CRITIC with linguistic D numbers for blockchain platform evaluation. Eng Appl Artif Intel 2021;101:104200. doi: https://doi.org/10.1016/j.engappai.2021.104200.

[59] Albahri OS, Zaidan AA, Albahri AS, Alsattar HA, Mohammed R, Aickelin U, et al. Novel dynamic fuzzy Decision-Making framework for COVID-19 vaccine dose recipients. J Adv Res 2022;37:147–68. doi: https://doi.org/10.1016/j.jare.2021.08.009.

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

[61] Senapati T, Yager RR. Fermatean fuzzy weighted averaging/geometric operators and its application in multi-criteria decision-making methods. Eng Appl Artif Intell 2019;85(March):112–21. doi: https://doi.org/10.1016/j.engappai.2019.05.012.

[62] Senapati T, Yager RR. Some new operations over Fermatean fuzzy numbers and application of Fermatean fuzzy WPM in multiple criteria decision making. Informatica 2019;30(2):391–412.

[63] Aydemir SB, Yilmaz Gunduz S. Fermatean fuzzy TOPSIS method with Dombi aggregation operators and its application in multi-criteria decision making. J

Intell Fuzzy Syst 2020;39(1):851–69. doi: https://doi.org/10.3233/JIFS-191763.

[64] Mishra AR, Rani P. Multi-criteria healthcare waste disposal location selection based on Fermatean fuzzy WASPAS method. Complex Intell Syst 2021;7(5):2469–84. doi: https://doi.org/10.1007/s40747-021-00407-9.

[65] Gül S. Fermatean fuzzy set extensions of SAW, ARAS, and VIKOR with applications in COVID-19 testing laboratory selection problem. Expert Syst 2021;38(8):1–16. doi: https://doi.org/10.1111/exsy.12769.

[66] Mishra AR, Rani P, Pandey K. Fermatean fuzzy CRITIC-EDAS approach for the selection of sustainable third-party reverse logistics providers using improved generalized score function. J Ambient Intell Humaniz Comput 2022;13(1):295–311. doi: https://doi.org/10.1007/s12652-021-02902-w.

[67] Rani P, Mishra AR. Fermatean fuzzy Einstein aggregation operators-based MULTIMOORA method for electric vehicle charging station selection. Expert Syst Appl 2021;182(February):. doi: https://doi.org/10.1016/j.eswa.2021.115267115267.

[68] Saraji MK, Streimikiene D, Kyriakopoulos GL, Tvaronaviciene M, Fermatean fuzzy CRITIC-COPRAS method for evaluating the challenges to industry 4.0 adoption for a sustainable digital transformation, 2021, doi: 10.3390/su13179577.

[69] Liu D, Liu Y, Wang L. 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 2019;34(11):2807–34. doi: https://doi.org/10.1002/int.22162.

[70] Elomda BM, Hefny HA, Hassan HA. An extension of fuzzy decision maps for multi-criteria decision-making. Egypt Inf J 2013;14(2):147–55.

[71] Joshi D, Kumar S. Intuitionistic fuzzy entropy and distance measure based TOPSIS method for multi-criteria decision making. Egypt Inf J 2014;15(2):97–104.

[72] Alsattar HA, et al., 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*, 2022;1–41.

[73] Salih MM, Al-Qaysi ZT, Shuwandy ML, Ahmed MA, Hasan KF, Muhsen YR. 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 2022;43(3):3549–59. doi: https://doi.org/10.3233/jifs-220707.

[74] Al-Hchaimi AAJ, Sulaiman NB, Mustafa MAB, Mohtar MNB, Hassan SLBM, Muhsen YR. Evaluation approach for efficient countermeasure techniques against denial-of-service attack on MPSoC-based IoT using multi-criteria decision-making. IEEE Access 2023;11:89–106.

[75] Experimental modeling and optimization of surface quality and thrust forces in drilling of high strength Al 7075 alloy: CRITIC and meta heuristic algorithms. [Online]. Available: https://link.springer.com/article/10.1007/s40430-021-02928-3.

[76] Albahri OS, Zaidan AA, Salih MM, Zaidan BB, Khatari MA, Ahmed MA, et al. 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 2021;36(2):796–831. doi: https://doi.org/10.1002/int.22322.

[77] Abdulkareem KH, Arbaiy N, Zaidan AA, Zaidan BB, Albahri OS, Alsalem MA, et al. 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 2021;33(4):1029–54. doi: https://doi.org/10.1007/s00521-020-05020-4.