Implementation Dual Parallelism Cybersecurity Architecture on FPGA

Nada Qasim Mohammed[1], Amiza Amir [1], Muataz Hammed Salih[2], Hana Arrfou[3], Qasim Mohaammed Hussein[4], and Badlishah Ahmad[1]
[1] Advanced Computing (ADVCOMP) CoE, Faculty of Electronic Engineering Technology University Malaysia Perlis (UniMAP), Arau, Malaysia
[2] IR4.0 and Intelligent Automation Group, Design and Engineering, Flex, Penang, Malaysia
[3] School of Business administration, Community Collage of Qatar, Doha, Qatar
[4] Tikrit University, Salah Adin, Iraq
Email: nadaqasim99@gmail.com; amizaamir@unimap.edu.my ;muataz.aldoori@flex.com; hana.arrfou@ccq.edu.qa ; kassimalshamry@yahoo.com

Abstract —This paper presents an efficient parallelism architecture that uses a dual-computing engine architecture to better throughput using both spatial and temporal parallelism on FPGA technology. This architecture will enhance the performance in terms of operating frequency and throughput and reduces the power consumption that meets applications with huge data processing such as Internet of Things .in this design, two boards are used, "DE1_Soc and NEEK board" with Altera Quartus Prime 18 for synthesis and simulation. The proposed design architecture gives better resource usage and throughput through fewer hardware redundancies using a frequency of 600MHZ with 64 bits for each engine from the dual-engine. Furthermore, the proposed architecture implementation results show the reduction in the time delay by 40 % and achieves a throughput of 153.6 Gb/s

Index Terms—Field programmable gate array, embedded system design, spatial parallelism, AES encryption/decryption, Low power Architecture, Internet of thing

I. Introduction

In this digital age, cyberspace has become an arena for Management, social services, education, marketing, business, and entertainment in everyday life. This was accompanied by an increasing in threats and breaches cybersecurity to access, steal, damage, or change the information or during storage or transmission over networks [1]. To secure these data need executing complex cybersecurity algorithms, such as AES algorithm, that requires high computing power, which makes sequential processing inefficient. Therefore, it is necessary to use parallel processing to execute these algorithms to obtain the most conceivable computational power of operations and throughput [2]. Various approaches have been introduced to deal with the complex computation problem to achieve low cost in hardware (area and power consumption) and high-speed performance. One approach is to invest parallelism in the spatial domain to perform tasks in parallel execution by using several processing units to use parallel features of functional units. This parallelism will take less time to execute the processing of operations; the most important features that should be considered when choosing parallel processing are reconfigurability, cost, power consumption, and time processing [3], [4].

Field-programmable gate arrays (FPGAs) have most of these features and more characteristics, which are suitable for implementing architectures with high parallelism, reliability, and flexibility [5]. In concern of security, cryptography plays a vital role in protecting information in cybersecurity protection. High-security cryptography algorithms that achieve information secrecy and integrity require high computational capabilities to increase the speed of operation and throughput. For example, AES is a good cryptography algorithm to ensure cybersecurity, and there is no practical attack against it [6]. Nevertheless, this algorithm requires high computational power to execute its operations. Therefore, a significant amount of research has been conducted on hardware implementation of the AES algorithm using FPGA. These implementations on hardware aim to achieve increased throughput and operating frequency, in addition to lower power dissipation, decreased latency and less area occupation

In this study, a hardware implementation of an efficient architecture is performed on the FPGA using spatial and temporal parallelism to obtain better throughput with a high operating frequency and fewer hardware redundancies. DE1 and neek-board devices are used in designing and implementing a dual-computing engine architecture using spatial and temporal parallelism. In this architecture, each color image is split into two equal parts, and each part is executed in one of the two engines concurrently. Deep pipelining is used to execute instructions of each engine independently. Encrypted color images using the AES cryptography algorithm were adopted to implement the proposed architecture". The remainder of this paper is organized as follows. in section 2 the literature survey is presented. Section 3 discusses the system specifications for the hardware implementation of the proposed architecture. Section 4

Manuscript received October 8, 2021; revised April 14, 2022.
doi:10.12720/jcm.17.5.386-392

provides the results and discussion, and Section 5 includes concludes of this paper

II. Literature Survey

Various architectural designs have been implemented on FPGA families to achieve many advantages, such as increased operating frequency, better throughput, decreased latency, lower power dissipation and lesser area, these approaches aim to optimize the power and increase the processing speed for many algorithms and applications. For example, several studies proposed a memory-based architecture design with less time and less complex. However, these architectures design requires more access time and more area, in addition to consumes more power [7]-[9].

In [10], the authors] proposed a mathematical and analytical model of the application's throughput in real time, using a low-latency Bloom filter on an FPGA, to obtain high-performance real-time information. In [11], a hardware design for the AES algorithm using a pipelined architecture was introduced. It delivers 2.29 GB/s encryption throughput at 56 MW of power consumption in 0.18-μm CMOS technology.

Partial parallelism to perform a fully stochastic simulation using FPGA architecture has been harnessed by [12]. As a result, the architecture, which presented, is faster than the existing simulator designed and implemented using FPGA with over 12-30 times that meet design requirements. Furthermore, to reduce the area of the crypto core, AES encryption and decryption were combined in [13]. from literature survey, one can conclude that memory-based architecture and combinational logic models consume more power and occupy more areas. In contrast, a composite field such as the Galois field model consumes significantly less power.

In [14], the author proposed FPGA architecture for parallel connected components analysis. It is based on partitioning the image into several vertical image slices, each slice processed in parallel. They used a coalescing unit collects information of components spanning these slices.

To produce high accuracy and throughput, Min, J. J., Salih, M. H eta al proposed new embedded data acquisition unit using spatial parallelism on DE0-Nano Field Programmable Gate Array board. In this proposal, through spatial parallelism, Up to 7 input channels processed concurrently. The design of the system increases the operating frequency up to 1GHz. [15], [16] introduced the design of an AES algorithm using Xilinx SysGen, implemented on Nexys4, and simulated it using Simulink. It consumes 121 slice registers, and its operating frequency is 1102.536 MHz, and the system throughput is 14.1125 Gbps. MATLAB was used to generate keys. In [17], proposed approach sub-kernel parallelism that based on the correlation between execution semantic of FPGAs and OpenCL parallelism abstraction to decouple the actual computation from data access of memory. This overlaps the computation of current threads with the memory access of future. The achieving of implementing this kernel parallelism is 7% increase in power consumption which increases the speed 2X and reduces the overall energy consumption more than 40%., with only 3% increase in utilization of resources. In [18], Neelima and Brindha elaborated a parallelism architecture using the Quartus FPGA device to explore the parallelism within the mix column in the AES algorithm. This architecture reduces the area by 30% and a 5% delay. Graded and Deshpande [19] discussed a composite field arithmetic SBOx to improve the delay performance. In their work, composite field arithmetic AES SBox, pipelined SBox, LFSR-based SBox and direct compute SBox were presented. In [20], a triple-key AES on a Spartan 3E FPGA kit was proposed. The researchers mentioned their results to optimize the delay of 4.221ns in the outcome and 1.55w in total power consumption.

[21] used the entire pipeline and parallel computing features of the FPGA to optimize the high-performance AES encryption algorithm. Then, [22] proposed pipeline techniques to implement the AES algorithm on an FPGA to increase the AES encryption speed. They used the Xilinx "Spartan-3A/3AN FPGA Starter Kit to implement the AES algorithm. The implementation results of the proposed algorithms were good.

In [23], the proposed implementation of the AES] algorithm on FPGA uses a multistage pipeline and resource sharing to secure and provide low power and area for networks of IoT applications. Meanwhile, the authors in [24] proposed an architecture on the Xilinx Spartan FPGA series to implement AES-128 to minimize the area and reduce hardware utilization. From the obtained results, the reduced area was 67%, and the delay increase was 69%.

In [25], the authors presented a high performance computing architecture that exploited FPGAs as "full-fledged peers" within a distributed system instead of attached to the computer central processing. The resultant of hardware implementation gives improves the latency to 25% versus a software-based transport, the computing throughput increased 10%.

In order to get high-performance computing domain, the authors presented a workflow for semi-optimal FPGAs for network structure applications by takes advantage of the FPGA key characteristics. They implemented their design for three representative applications on a Xilinx Alveo U280 FPGA. The implementation using the low-level circuit elements results showed 2× energy savings [26].

In [27], Authors introduced lightweight block cipher architecture to ensure security against attacks of malicious that make used of pseudo random number with good random statistical features This architecture utilizes dual-port read-only memory to generate the 80-bit key from 64-bit of input. The operating frequency of the generator architecture was 612.208 MHz using a Virtex 5

III. Spatial and Temporal Parallelisms

Data partitioning strategies significantly aid in data processing techniques to improve performance by using parallel processing systems [28]. Spatial parallelism allows duplication of tasks that can be processed via specific modules using many engines. These tasks were performed simultaneously in different physical locations. In the spatial parallelism mechanism, the main task is divided into several regions, and then each region is processed by processing element independently [29]. This hardware duplication reduces the processing speed and increases throughput by processing multiple tasks at times. Therefore, using spatial parallelism as a solution merits attention to process many tasks simultaneously via different processing models unless there are no resource conflicts. Significantly, the flexibility of spatial computation performance is available in reconfigurable platforms [30]. The spatial parallelism features are explored and used at many construction levels of the system, starting with the system interconnection to the entire functional unit features to improve the system's throughput. Therefore, it is considered as a potential solution in parallel system design, and many techniques use spatial parallelism techniques to execute complex algorithms; one explores the parallelism features on FPGA. [5].

In temporal parallelism can be used pipelined to reduce the total cycle's number to process the file, which makes the system faster. Also in the case, the number of system cycles will reduce by using the parallel processing technique which is based make the processor work as more than one processors to achieve the task processing faster as possible.

IV. The Proposed Architecture

The proposed architecture is designed to work with efficient parallelism that able us to use it for any image processing process by modifying only small part of it. the details of it as following:

A. Architecture Specifications

The top-level design of the proposed system, presented in Figure "1", illustrates the design of dual engine cybersecurity computing architecture using a spatial parallelism and a temporal parallelism on an FPGA, depends on using a DE1_SoC board connected with a NEEK board through Wi-Fi in each DE1_Soc (Server) and NEEk board (Client).

The presented design implement makes use of the spatial parallelism on the FPGA technique for processing, simultaneously, four parts of the input image; each performs a specific function.

The architecture consists of three parts, which are explained in detail, Fig. 1.

- SD cards: The design used a Micro SD card interface to read and store the reading images.SD card is 2 Gb for NEEK board and 4Gb for DE1_SoC.
- Two engines: They process the data in parallelism manner simultaneously. The engine consists of the necessary operation of the encryption/decryption processing unit, on-chip mem, sync, and time/multi-clock units. The processing in each engine depend on using pipelining architecture.
- The Wi-Fi controller transfers images between two boards: DE1-SoC and NEEK boards. Both boards had the same TLDs. Wi-Fi in DE1_SoC operates as (Server) and Wi-Fi in NEEK operates as (Client), so the transmission will be easy.

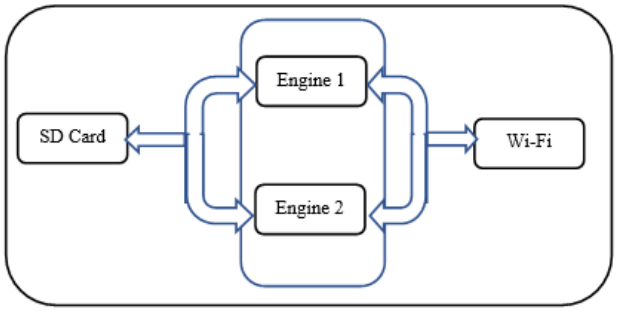


Fig. 1. Architecture main parts

B. Engine Top Level Design

Each engine includes five Part. This section explains in detail the top-level design of each machine, as shown in Fig. 2. The design contains the following parts:

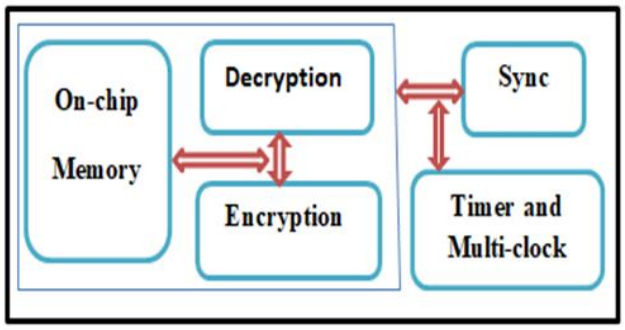


Fig. 2. Engine top-level design

- On-Chip Memory: The DE1-SoC computer includes a 256 KB memory that is implemented inside the FPGA chip, which organized into 64 K × 32 bits. Memory is used as a pixel buffer for storing the image when encrypting and storing the image during decryption.
- Encryption/ decryption: This part performs the encryption or decryption process programs depending on the aim of the execution. The symmetric block cipher AES was used to encrypt the images. In AES, all arithmetic operations are performed over a finite field GF(28). It takes a key length of 128 bits and 128 bits' plain text block size.
- Sync: This part of the design uses the timer scheduler of all operations/tasks inside each engineer, and uses master and multi block

generators to synchronize all transmissions.

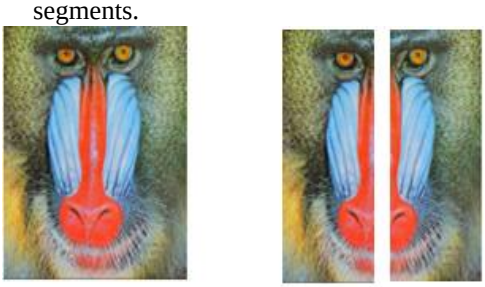
- Timer and multi clock: This part generates the necessary clocks and timers for different operations. Some of the subunits work with different watches, such as 1GHz, 1.3GHz, and 600MHZ. Sub-units are those in TLD and use different frequencies

C. Images Encryption Process

To encrypt the image, or any type of image processing, the following steps are performed:

Image's preparing: This step includes two steps. The first step is reading the image. Images have different types of gray or color of any size. After reading, the image will be split vertically into two equal segments, as Fig. 3.

- Each segment is transferred to one of the two images.
- Each engine executes the encryption/ decryption process using AhghggES-128 bit simultaneously.
- After finishing the encryption/ decryption process, the processed data return to SD card and store these data after merging the two segments.



(a) Original Image (b) Image Splitting

Fig. 3. Image splitting operation

D. Image Decryption Process

To decrypt the encrypted image as in Fig. 1, the same steps are repeated in 3.3, except there is a changing in the function of the encoder/decoding part, where the program that related to the decryption process is executed

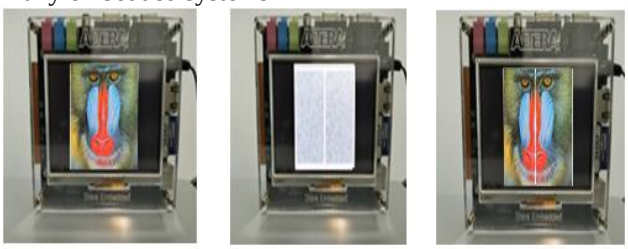
V. Implementation and Results Analysis

The proposed design is implemented on DE1_Soc(server) and NEEK board(client) connected using Fi-Wi on both boards, and the software is Altera Quartus Prime 18 for synthesis and simulation. The AES version is a 128-bit block used to encrypt images. Firstly, before encryption process, each image is divided into two equal parts, and each two parts are processed by one engine of the architecture. After processing the image, the next image will be read. Each part is processed in 1.66 * 10^{-6} seconds. Fig. 4 include original images examples and their encrypted and decrypted by using spatial and temporal parallelism with dual engines

Through the results obtained from the implementation of the architecture, the application of the spatial parallelism principle can enable modules of the system to process multiple input data at the same time to achieve multiple outputs, thus decreasing the complexity of overall system and increasing the utilization of the module. After executing the proposed architecture implementation, the final results were displayed on the LCD touch screen.

The experimental results show the architecture efficiency in terms of increasing the processing speed and high throughput. In contrast, NEEK showed the desired results even there is a noise was present within the input system signals Furthermore, one can be concluded that spatial parallelism is a good solution for systems that require real-time processing features, especially embedded system

In this paper architecture, one can overcome some issues that faces systems resources constrains, such as memory size within the system, speed, and power consumption represent real challenge, which are faced many embedded systems



(a)Original Image (b)Encryption Image (c)Decryption Image

Fig. 4. Encryption and decryption processes

The hardware implementation results were shown that the throughput become153.6 Gb/s which is faster than the results obtained from implementation this system using software. The proposed system supported with the ability to flexibility, reconfigurability, and reliability of the FPGA

The novelty of the proposed algorithm can be summed up in the following: Achieve the parallelism in two approaches spatial and temporal. In the spatial domain, it creates multiple engines to handle different files at the same times. Whereas in temporal domain, it uses deep pipelining by dividing every engine to sub modules to process and execute different executing tasks. In the security part, the dividing/encryption/decryption /collecting of files remain as original with minimum data corruption

Table I: Comparison with Others Work for Frequency and Throughput

Design	Device	Frequency MHz	Throughput (Mbps)
Our architecture	SoC and Neek board	600	153.6 Gbps
[11]	a Virtex-II	159.210	1.941
[16]	Nexys4 Xlinix	112.536 MHz	14.1125 Gbps
[19]	Virtex-4 XC4VLX200	112.37	14,383
[20]	Spartan 3E FPGA kit	77.6	867.34
[24]	Spartan-3 XC300s	67.75	8672

VI. Conclution

This study demonstrates the ability of the proposed architecture to perform the AES algorithm in spatial and temporal parallelism with high productivity. Within the Altera® Nios "II" Embedded Evaluation Kit, Cyclone "III" Edition many good features was harnessed to implement our design of this paper, such as the LCD touch screen, the switch inputs and "LEDs".

The implementation results conformed high throughput of the system for different frequencies with a maximum frequency of 600 MHZ with 64 bits in each engine with a throughput equal to 76.8 Gb/s, which means that the throughput will become153.6 Gb/s in all systems,

Therefore, the power consumption of the proposed design was significantly less. It can make use of these frequencies processing to be sent to platforms for IoT devices, which is defused, and shown on the LCD touch screen. All these results can be done with a resource utilization of low hardware.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

A, B, C construct the architecture that it achieves.
B, D, E get the analyzed data
A, B, C, D, E, F testing the result on different image
The authors approved the final version.

Acknowledgement

This work was not funded by any part. I would like to thank my supervisors Dr.Amiza Amir and Dr..Muataz Hameed , UniMAP staff, my family, and everyone who supported me to make this work

References

[1] G. O. Sapti, Q. M. Hussein, and Z. T. M. Al-Ta'I, "Q-NTRU cryptosystem for IoT applications," J*ournal of Southwest Jiaotong University*, vol. 54, no. 4, 2019.

[2] M. N. Qasim, H. Q. Mohammed, M. S. Ahmed, and A. K. Layth, "A hybrid approach to design key generator of cryptosystem," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 3, pp. 971-977, March 2019.

[3] N. Q. Mohammed, M. H. Salih, R. Aliana, Q. M. Hussein, and N. A. A. Khalid, "Design and implementation Image Processing functional units using spatial parallelism on FPGA," *ARPN Journal of Engineering and Applied Sciences*, vol. 13, no. 15, pp. 4514-4520, 2018.

[4] R. M. Aldahdoo, "Parallel implementation and analysis of encryption algorithms," Master thesis, Al-Azhar University-Gaza, 2018.

[5] N. Q. Mohammed, M. H. Salih, R. Aliana, Q. M. Hussein, and N. A. A. Khalid, "FPGA implementation of multiple processing algorithms using spatial parallelism," *ARPN Journal of Engineering and Applied Sciences*, vol. 13, no. 15, pp. 4556-4562, 2016.

[6] W. Stallings, *Cryptography and Network Security Principles and Practice*, Seventh edition, published by Pearson Education Limited, 2017.

[7] T. Good and M. Benaissa, "Very small FPGA application-specific instruction processor for AES," *IEEE Trans. Circuits System*, pp. 1477–1486, 2006.

[8] H. Zodpe and A. Sapkal, "An efficient AES implementation using FPGA with enhanced security features," *Journal of King Saud University – Engineering Sciences*, vol. 32, pp. 115–122, 2020.

[9] C. T. Chow, L. S. M. Tsui, P. S. Leong, W. Luk, and J. S. E. Wilton, "Dynamic voltage scaling for commercial FPGAs," in *Proc. IEEE International Conference*, 2005, pp. 173-180.

[10] S. R. Chalamalasetti and M. Margala, "Throughput analysis for a high-performance FPGA-Accelerated real-time search application," *International Journal of Reconfigurable Computing*, 2012.

[11] M. S. Kumari, D. M. Kumar, and Y. R. Devi, "High throughput-less area-efficient FPGA Implementation of block cipher AES algorithm," in *Proc. International Conference on Advanced Computing, Communication and Networks*, 2011, pp. 484–489

[12] B. T. David and A. Hideharu, "A fully pipelined FPGA architecture for stochastic simulation of chemical systems," in *Proc. IEEE 23rd International Conference on Field Programmable Logic and Applications *FPL*,* Portugal, 2013.

[13] M. R. Rao and R. K. Sharma, "FPGA implementation of combined AES-128," in *Proc. 8th International Conference on Computing, Communication and Networking Technologies*, 2017.

[14] M. J. Klaiber, D. G. Bailey, S. Ahmed, Y. Baroud, and S. Simon, "A high-throughput FPGA architecture for parallel connected components analysis based on label reuse," in *Proc. International Conference on Field-Programmable Technology*, 2013.

[15] J. J. Min, M. H. Salih, Z. Ng, T. Kho, Y. S. Woo, and F. Yee, "Design and implementation of embedded DAQ using spatial parallelism on FPGA for better throughput," in *Proc. 3rd International Conference on Electronic Design*, 2016.

[16] P. B. Mane and A. O. Mulani, "High-Speed area efficient FPGA implementation of AES algorithm," *International Journal of Reconfigurable and Embedded Systems*, vol. 7, no. 3, pp. 157-165, November 2018.

[17] S. A. Shiddibhavi, "Empowering FPGAS for massively parallel applications," Mater thesis, The University of North Carolina at Charlotte, 2018.

[18] S. Neelima and R. Brindha, "FPGA-Based implementation of AES algorithm using MIX column," in *Microelectronics, Electromagnetics and Telecommunications. Lecture Notes in Electrical Engineering*, J. Anguera, S. Satapathy, V. Bhateja, and K. Sunitha, Eds., Springer, Singapore., 2018.

[19] M. Wong, M. L. D. Wong, C. Zhang, and I. Hijazin, "Circuit and system design for optimal lightweight AES encryption on FPGA," *IAENG International Journal of Computer Science*, 2018.

[20] F. Noorbasha, Y. Divya, M. Poojitha, K. Navya, A. Bhavishya, K. K. Rao, and K H. Kishore, "FPGA design

and implementation of modified AES based encryption and decryption algorithm," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, pp. 132-136, 2018.
[21] H. Y. Chen and S. C. Yu, "FPGA implementation and design of a hybrid Chaos-AES color image encryption algorithm," *MDP Journal*, vol. 12, no. 2, 2019.
[22] M. Nabil, A. A. M. Khalaf, and S. M. Hassan, "Design and implementation of pipelined and parallel AES encryption systems using FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, pp. 287-299, 2020.
[23] P. Rajasekar and H. Mangalam, "Design and implementation of power and area optimized AES architecture on FPGA for IoT application," *Circuit World*, vol. 47, no. 1, 2020.
[24] C. A. Murugan, P. Karthigaikumar, and S. S. Priya, "FPGA implementation of hardware architecture with AES encryptor using sub-pipelined S-box techniques for compact applications," *Journal for Control, Measurement, Electronics, Computing and Communications*, vol. 61, no. 4. pp. 682–693, 2020.
[25] J. Lant, J. Navaridas, M. Luján, and J. Goodacre, "Toward FPGA-Based HPC: Advancing interconnect technologies," *IEEE Micro*, vol. 40, no. 1, pp. 25-34, 2020.
[26] K. Kamalakkannan, I. Z. Reguly, and S. A. Fahmy, "High-Level FPGA accelerator design for structured-mesh-based explicit numerical solvers," arXiv:2101.01177v2 [cs.AR], Jan. 2021.
[27] T. Kowsalya, R. G. Babu, B. D. P. Chari, A. Nayyar, and R. M. Mehmood, "Low area PRESENT cryptography in FPGA using TRNG-PRNG Key generation," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 1447-1465, 2020.
[28] C. Zhao, Y. Zhao, L. Meng, *et al*., "The key technological issues of parallel spatial database management system for parallel GIS," *Computer Knowledge & Technology*, vol. 47, no. 4, pp. 1265-1270, 2005.
[29] B. R. Kumar, K. Deepak, and K. S. Pandey, "Concept, design and performance evaluation of VLVIW processor," *International Journal of Scientific Engineering and Technology*, vol. 2, no. 7, 2013.
[30] O. F. Yousif, M. H. Salih, L. A. Hassnawi, *et al*., "Design and implementation computing unit for laser jamming system using spatial parallelism on FPGA," in *Proc. IEEE International Conference on Signal and Image Processing Applications*, 2015.

Nada Qasim Mohammed received the B.S. degree in computer engineering from Baghdad University, Baghdad, Iraq, in 2009, and the M.S. degree in Embedded System Design Engineering from University Malaysia Perlis, in 2016. She is currently pursuing a Ph.D. degree in computer engineering with the University of Perlis, Malaysia. His current research interests include Cybersecurity, the internet of thing, system architect, designing digital systems using FPGA systems, and computer system architecture

Amiza Amir received her Ph.D. in Artificial Intelligence from Monash University, Melbourne, Australia in 2015. She is currently a senior researcher at the Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis. She is also a fellow researcher at the Advanced Computing (ADVCOMP) Center of Excellence. Her current areas of interest include distributed computing, machine learning, data analytics, swarm-based optimization, and software-defined network (SDN). Dr. Amiza published a number of papers in preferred journals and chapters in books and participated in a range of conferences on information technology.

Muataz Hameed Salih (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from the Dept. of Computer Engineering from University of Technology, Iraq, in 1998 and 2002, respectively. In Sept 2013, he earned a PhD degree in Computer Engineering, with specialization in FPGA Embedded Multiprocessor SoC. From Sept. 1998 to March 2003, he was a research engineer in Military Industrialization Corporation of Iraq. From Oct. 2003 to June 2008, he was a lecturer and manager of the engineering faculty's LABS in the faculty of Engineering of Al-Kalamoon private university, Syria. From July 2008 to July April 2011, he was a Researcher at the Underwater Robotic Research Group at USM. Nov. 2013 to Oct 2018, he is a Senior lecturer at UniMAP, Malaysia. Since Oct. 2018, he is an FPGA Senior Staff Manager at Flex company. He is IR4.0 and Intelligent Automation lead of Flex Penang Cluster. He is SMIEEE, CEng, MIET, and IACSIT Senior Member. His research interests and working area on Multiprocessors SoC design, system architect, designing digital systems using FPGA technology, FPGA-SoC design, embedded systems, computer system architecture, microprocessor architecture, an active jamming system or laser missiles, IR4.0 transformation, Cybersecurity and Intelligent Automation.

Dr. Hana Arrfou received her Bachelor's degree in Computer Science in 2009 from Al-Hussein Bin Talal University- Jordan and received a Master's degree in Electronic Business Administration in 2012 from Mutah University - Jordan. In 2017, She obtained a Ph.D. in Production and Operations Management from the University Malaysia Perlis – Malaysia. She is currently an assistant professor in the Community College of Qatar. Her research interests are in supply chain quality management with technological capability and lean manufacturing practice.

Prof. Qasim Mohammed Hussein has PhD degree in computer sciences from Technology University and is currently Professor at Tikrit University. He published 33 journal articles in the fields of cryptography and computer security, He participated in writing (5) books in computer science, registering in the Iraqi national library – the house of books and documentations. He reviewed dozens of scientific researches to scientific upgrade in Iraq universities or for publication in the scientific journals, and

a member of the preparation and scientific committees for scientific conferences. He was a member of the editorial board of Journal of Pure Science at the University of Tikrit, an expert in many committees, and contributed to a number of scientific and preparation committees of scientific conferences. He attended many conferences and scientific symposia, inside and outside of Iraq, and has a number of lectures and field studies in the field of computer.

R. Badlishah Ahmad (Senior Member, IEEE) received the B.Eng. degree (Hons.) in electrical and electronic engineering from Glasgow University, in 1994, and the M.Sc. degree in optical-electronic engineering and the Ph.D. degree from the University of Strathclyde, in 1995 and 2000, respectively. He is currently a Professor at the Faculty of Electronics Engineering Technology, UniMAP. His research interests are in computer system and telecommunication network modeling using discrete-event simulators, optical networking, and embedded system based on GNU/Linux.