2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW) | 979-8-3503-0208-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/CCGridW59191.2023.00031

RISC-V Core for Ethical Intelligent IoT Edge: Analysis & Design Choice

Haribabu P, Sasirekha GVK, Madhav Rao, Jyotsna Bapat, Debabrata Das

CIET, International Institute of Information Technology
Bangalore, India

{haribabu.pasupuleti, sasirekha,mr,jbapat, ddas}@iiitb.ac.in

***Abstract*—With the wide deployment of Internet of Things (IoT) solutions, along with the increased demand for incorporating intelligence at the edge, the development of high-performance System-on-Chips (SoC), specifically for edge devices, has gained momentum. Currently, most of the processors used for the development of IoT edge device are ARM architecture based, where license fees are involved. An open-source RISC-V based SoC for IoT edge is the requirement of the day that will accelerate IoT development and widespread deployment. This open-source RISC-V based device needs to be secure and protected from privacy breaches. The first and most crucial step towards developing such a secure and privacy enhanced ethical SoC for the edge, is the choice of RISC-V core. In this paper, the analysis performed for the design choice of the RISC V processor core has been detailed. After surveying the literature, three cores have been shortlisted and synthesized using FPGA device of Virtex®UltraScale+ family from Xilinx. The inferences from the synthesis results and its impact on the architecture of the proposed IoT edge SoC have been presented. The challenges in the design of an ethical edge-IoT SoC have been described. The approach for implementation and evaluation has been discussed.**

Keywords*—*Internet of Things (IoT), Edge, RISC-V, Field Programmable Gate Array (FPGA), ARM, System-on-Chip (SoC), IoT processor.

I. INTRODUCTION

In recent years, tremendous growth in Internet of Things (IoT) applications that utilize cloud computing and storage has been seen. The major challenges in developing cloud based smart IoT systems is the management of the vast amount of data, while maintaining the real-time performance. Ethics of the data is another critical factor of IoT, which defines the brand and trust of the organizations involved in providing the IoT services. Ethical use of data can be addressed by privacy and security, along with the policies. Edge based computing helps handle the data processing and analysis locally, thus enhancing the performance with respect to latency and bandwidth. In addition, edge devices manage the ethics better because of localization, which ensures reduced data exposure, implying lesser number of security and privacy breaches. Thus, because of the increasing role edge devices in improving the performance of cloud based IoT systems, the System on Chip (SoCs) used for this edge platform has become a crucial design element [1, 2].

The SoC used on the edge device needs to be low cost, manage large volumes of real-time data ethically. It implies that it should provide security and privacy, along with machine learning capabilities for intelligence. It also needs to provide for the required interfaces for handling images, audio and video streams of data. Edge devices can be further categorized into two classes. Class 1 are tiny or thin devices that consume less power and operate on batteries that last over years. The type of connection to the external environment of class 1 devices is through simple sensors or actuators, like temperature, pressure, relay, etc. Such class 1 edge nodes are used to connect legacy equipment to their cloud solutions, for example, track and trace, agricultural monitoring, smart buildings, etc. These use cases transmit low-volume data to the centralized monitoring and management platform. Class 2 edge devices, on the other hand, need to support high speed interfaces for video, audio, and image data, in addition to the simple sensors and actuators. They constitute thick edge hardware, supporting advanced on-device inference, event processing rules, business logic, analytics, and machine learning algorithms, for example a smart factory.

The five basic building blocks of IoT edge device hardware are, i) Processor, ii) Sensor/actuator interface, iii) Storage, iv) Power source or converter, and v) Communication transceiver. With the advances in VLSI design and fabrication technologies, more and more blocks are getting integrated into single SoC, to ensure the reduction of edge device area and power consumption. The adoption of RISC-V, a free and open-source computer ISA has been trending as the core for the SoC processor, mostly because of the Artificial Intelligence (AI) and Machine Learning (ML) requirements. RISC-V is an open Instruction Set architecture (ISA) that scales from 16-bit to 128-bit register platforms. RISC-V accelerates AI with relatively low power consumption. For example, the ET-SoC-1 was designed to accelerate AI in power-constrained data centers, as the heart of boards that fit into the Peripheral Component Interconnect express (PCIe) slot of already installed servers. RISC-V is supported by compiler technologies like Generic C Compiler (GCC) and Low-Level Virtual Machine (LLVM) that can handle additional instructions. Low-power IoT applications can benefit from this approach by implementing some functions in hardware [3, 4].

In this paper, the architecture of an SoC that contains sensor interfaces for high data rate sensors, open instruction set processor which is compliant to open RISC-V architecture, light weight cryptographic sub-block, Homomorphic Encryption (HE) engine, and Machine Learning (ML) accelerator is proposed. The work focusses on the first step towards the development of an SoC, that is the analysis and choice of RISC-V core for the proposed architecture. The literature survey on the recent work on IoT SoCs have been discussed in section II. Open-source synthesizable cores and their synthesis results, along with inferences are discussed in section III. Section IV presents the proposed architecture with the shortlisted core. Section V contains the challenges involved in developing the secure,

979-8-3503-0208-0/23/$31.00 ©2023 IEEE
DOI 10.1109/CCGridW59191.2023.00031

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

private, edge SoC. Section VI discusses the conclusions and future work.

II. Related work on SoCs

Authors in [5] have developed and fabricated a hybrid architecture SoC consisting of a microcontroller, and a configurable logic cell block that connects to I/O peripherals. This configurable logic cells can be used for designing peripheral controller on the fly. This approach enables easy interfacing of various sensors and actuators. However, a detailed analysis of the peripheral controller power consumption needs to be performed, to evolve an optimum methodology for peripheral interfacing.

[6] discusses fabrication of a RISC-V ISA SoC with 0.18 um CMOS General Purpose (GP) technology and this is meant for a low data rate sensor interfaces like temperature, relative-humidity and barometric pressure. [7] presents an 8-bit and 32-bit based SoC in a GPCMOS technology. The two processors are implemented in the same tape-out and with the same peripherals. Both of the processors are meant for low data rate sensor interfacing. In [8], authors have analysed open-source soft core processors and operating systems. It is seen that LEON3 and open RISC are two important platforms that can be used in the IoT field. Energy consumption analysis of these two systems were obtained and compared. FreeRTOS operating system has been installed and examined on the LEON3 processor. Thus, a technical analysis support for the mentioned platforms is provided to the designers.

Authors in [9] have presented design, implementation, and experimental verification of a smart sensor architecture, that satisfies the operational requirements needed by the Industrial Internet of Things (IIoT). Interoperability, high availability, synchronization, and local data processing have been validated from IIoT perspective. Further, encryption-decryption for cyber-security in the data link layer has been added and evaluated. [10] presents work on enabling the next generation of edge devices to process data from sensors capturing image, video, audio, or multi-axial motion/vibration data, involving high speeds and bandwidth. Challenges of running Convolutional Neural Networks (CNNs), in the constrained battery-powered IoT end-nodes, are discussed. GAP-8: a multi-GOPS fully programmable RISC-V IoT-edge computing engine, featuring an 8-core cluster with a CNN accelerator is proposed.

In [11], RISC-V core processor with RV32I subset instruction is used to build an AES cryptographic engine in an SoC. This core features separate instruction and a data bus using a Wishbone crossbar. [12] proposes an integrated cryptographic SoC architecture solution which provides security sub-modules, namely key exchange using Elliptic curve Diffie Hellman, management, and encryption/decryption. This architecture involves usage of a True Random Number (TRN) generator, CubeHash algorithm and AMBA AHB-APB bus, and PicoRV32 opensource RISC-V processor. The integrated architecture has been tested on Virtex 4 FPGA from Xilinx.

As a result of the study on the related work on SoCs using RISC-V, it is found that most of the work focussed on class 1 devices, or is specific to industrial IoT. The work in [10] addresses ML, but does not discuss the ethical aspects. [11, 12] integrate security, but not ML. It is observed that work for ethical and intelligent edge-IoT as a SoC, for class 2 use case, has not been investigated in open literature from the perspective of using RISC-V.

A genetic algorithm based approach for the choice of SoC for various IoT applications has been presented in [13]. Design space requirements of state-of-the-art processor core architectures and their corresponding CPU cores are implemented in Xilinx Zynq-7000 FPGA device and validated. This could provide a bench mark for future implementations like the one proposed in our paper.

III. Open source RISC-V synthesizable cores

A. Prior Art

The work done in [14] considers ten synthesizable processors that implement RISC-V ISA. The processors include 1) Roa Logic RV12 developed and maintained by Roa Logic [15], 2) ORCA designed and maintained by Vectorbox and was originally to serve as a host to Vectorbox's high-speed Matrix processor [16], 3) SiFiveE31 developed and maintained by SiFive [17], 4) SCR1, designed and maintained by Synatocore [18], 5) Rocket, developed and maintained by SiFive and the University of California Architecture Laboratory [19], 6) Berkeley Out-of-Order Machine (BOOM) is developed and maintained by Esperanto and the University of California Architecture Laboratory [20], 7) MRISCV designed and maintained by OnChipUIS [21], 8) PicoRV-32 developed and maintained by Clifford Wolf [22], 9) Shakti-E maintained by the Indian Institute of Technology (IIT) Madras [23], and 10) Hummingbird developed and maintained by Bob Hu from China [24]. The features for comparison were the i) ISA being RV321, RV641, or RV32MAC. ii) Architecture: Havard or Van Neuman iii) Datawidth: 32, 64, 32/64 bits iv) Pipeline depth v) Multiplier included vi) Divider included.

Further, these 10 cores were synthesized on FPGA and the results were presented in [14]. Results obtained synthesizing the ten processors, using the XC7Z020 FPGA device have been tabulated in [14]. The results include the maximum attainable operational frequency (Freq), the total number of Look Up Tables (LUTs), the total number of Flip-Flops (FFs), the total number of Block Random Access Memories (BRAMs), and Digital Signal Processors (DSPs). Resource utilization has been expressed as percentage of the total resources available. The codes of the processor core are available in five high-level languages which include VHDL, Verilog, SystemVerilog (SystemV), BluespecSystemVerilog (BSV), and Chisel. VHDL, Verilog, and SystemVerilog are HDLs that can be synthesized directly by the Vivado software. BSV and Chisel are higher-level languages that are converted to Verilog before synthesis is done.

B. Inferences and Synthesis results of shortlisted cores

The inferences from the synthesis of the 10 cores considered in [11] are: 1) PicoRV-32 has highest operating frequency of 200MHz. 2) Roa Logic has the 2nd highest operating frequency of 142.8 MHz. 3) PicoRV-32 consumes the least number of flipflops.4) PicoRV-32 consumes the least power. 5) SCR1 has the lowest speed of 40 Mhz among these 10 cores. Two high

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

Table I: Synthesis results of the three short-listed cores

Processor core	HDL	Freq (MHz)	LUT	LUTRAM	FF	Block RAM	DSP	Power (W)
Roa Logic	SystemV	143.5 (142.8)	4618 (3615)	0 (96)	3785, (2246)	1(0.5)	0 (0)	0.037
SCR1	SystemV	100 (40)	5178 (4337)	0 (1)	2837 (2143)	16 (0)	4 (1.82)	0.041
PicoRV-32	Verilog	200 (200)	894 (904)	48 (24)	615 (566)	0 (0)	0 (0)	0.013

Table II: XCVU9P versus XC7Z020 [14]

Feature	XCVU9 PL2FLGA2 104	XC7Z020
System logic cells (K)	2586	85
DSP slices	6840	220
Memory (Mb)	345.9	4.9
GTY/GTMTransceivers (32.75/ 58 Gb/s)	120/0	NA
I/O	832	200

frequency variants PicoRV-32 and Roa Logic, and low frequency variant SCR1 are considered for further synthesis on FPGA platformXilinx® Virtex®UltraScale+ XCVU9P-L2FLGA2104 device on VCU118 evaluation board. This choice is because one of the requirements is the high data rate sensor interface, for which a high frequency synthesizable core is essential. SCR1, the low frequency core is synthesized for bench marking the performance of other cores.

The syntheses report of the three shortlisted cores on the targeted FPGA are tabulated in Table I. Highlighted in red are the findings of [14]. These differences between the two synthesis reports are attributed to the difference in the capacity and architecture of the two different FPGAs used for synthesis. Table II shows the comparison between the FPGAs used. XC7Z020 device of Zynq7000 family is used in [14], whereas XCVU9P-L2FLGA2104 device of Virtex®UltraScale+ family from Xilinxis used for our synthesis.

Additionally, the resource consumption in terms of the high performance I/O, Carry 8 and global clock buffers have been compared in Fig. 1 for the 3 cores.

1) High-Performance I/O Banks (Bounded IOBs)

The I/Os in Xilinx 7 series FPGAs are classified as either High Range (HR) or High Performance (HP) banks. HR I/O banks can be operated from 1.2 Volts to 3.3 Volts. The High Performance I/O banks in the 7 series FPGAs can accommodate higher voltage interfaces via a series of options that can accommodate virtually all design, cost, and performance needs. Fig.1 shows that the IOB resources consumed by SCR1 is lesser as compared with Roa Logic and PicoRV-32.

2) Carry8

The carry chain consists of a series of eight MUXes and eight XORs that connect to the other logic (LUTs) in the CLB via dedicated routes to form more complex functions.

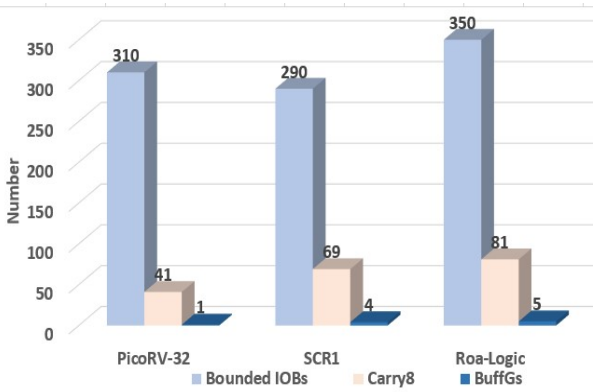

Fig1. Resources consumed by cores

The fast carry logic is useful for building arithmetic functions like adders, counters, subtracters, and add/subs, as well as other logic functions, such as wide comparators, address decoders, and some logic gates. This component can be used to operate as a single 8-bit carry or two independent 4-bit carry logic. Fig.1 shows that the carry logics utilised by PicoRV-32 is lesser than that of Roa logic and SCR1.

3) Global Clock Buffers (BuffG)

Global buffers are most used for clock nets to provide the least amount of skew. Skew occurs because of the registers being physically located large distances apart, on the chip. The design element is a high-fanout buffer that connects signal to the global routing resources for low-skew distribution of the signal. BuffGs are typically used on clock nets as well other High-fanout nets like sets, resets, and clock enables. Fig.1 shows that the global clock buffers used by the PicoRV-32 are lesser than that of the Roa logic and SCR1.

IV. PROPOSED IOT EDGE SOC ARCHITECTURE

The proposed architecture is illustrated in Fig.2. The design choice is PicoRV-32 as the core processor. PicoRV-32 core has been the choice because of the high-speed support and relatively lesser I/O blocks, carry8 and global clock requirements. Tentatively, AXI-lite as the communication protocol is being considered. AXI Lite is a simplified version of Advanced Extensible Interface (AXI) [25 and references therein]. The simplification has been achieved by removing the support for burst data transfers. AXI, in turn, is a revision of Advanced Microcontroller Bus Architecture (AMBA), wherein a point-to-point connectivity protocol has been introduced.

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

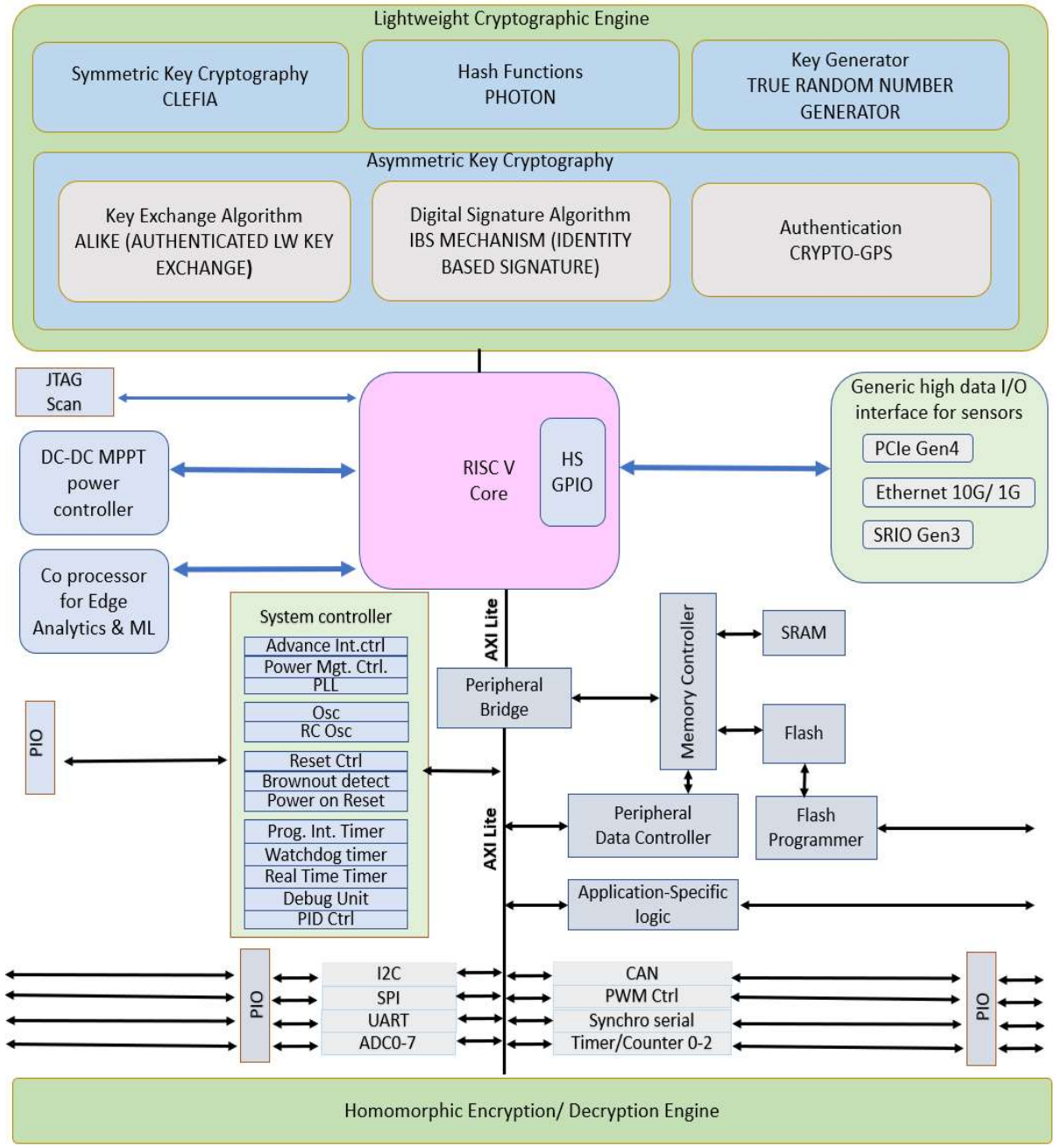

Fig.2. Proposed architecture for ethical intelligent IoT edge SoC

The choice of the standard bus protocol is crucial for building high performance SoC designs. Micro controllers or microprocessors, internal memory or external memory bridge, DSP, DMA accelerators, and various other peripherals like USB, UART, PCIe, I2C etc., communicate via the bus protocol. AMBA protocols have a standard and efficient way to interconnecting these blocks with re-use across multiple designs. AXI interconnect uses a master-slave protocol and is useful for high bandwidth and low latency interconnects. This is a point-to-point interconnect and overcomes the limitations of a shared bus protocol in terms of number of agents that can be connected. The protocol also is an enhancement from AHB in terms of supporting multiple outstanding data transfers (pipe-lined), burst data transfers, separate read and write paths, and supporting different bus widths.

A. Lightweight Cryptographic Module

In the resource constrained edge devices, there is a requirement of lightweight cryptographic algorithms, for providing security and privacy. Light weight implies low power, low area, and low cost. ISO/IEC 29192 [26] series pertains to light weight cryptography standardization effort by

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

ISO/IEC committee. There are totally '8' sub standards covering different aspects of light weight cryptography, such as data confidentiality, non-repudiation, identification, authentication and key exchange. Many of these standards are still under development. The ISO/IEC 29192-4 specifies key exchange protocol called ALIKE which is based on public key encryption scheme "RSA for Paranoids". The ISO/IEC 29192-5 standard specifies light weight Hash algorithms namely PHOTON and SPONGENT which are optimized for hardware implementations and LESAMNTA optimized for software implementations. Our proposal is to replace SHA family of algorithms in RBGs as specified in [SP 800-90] with light weight hash algorithms as specified in ISO/IEC 29192-5 for cryptographic key generation and adopting ISO/IEC 29192-4 for key exchange. Further, ISO/IEC 29192-2 and 29192-3 standards specify block ciphers (PERESENT, CLEFIA and LEA) and stream ciphers (ENOCORO and TRIVIUM) can be used for encryption and decryption of data packets/streams.

Hash functions constitute another important component of lightweight cryptographic algorithm standards. The standardized and widely-used MD5 (8001 GE), SHA-1 (5527 GE) and SHA-2 (10868 GE) and ARMADILLO (4353 GE) are too large to fit in hardware constrained devices (i.e. more than 3000 GE). After the release of the PRESENT cipher there were many efforts to build novel lightweight hash functions based on PRESENT design principles, like C-PRESENT (4600 GE), H-PRESENT (2330 GE) and PRESENT-DM (1600 GE). The newer lightweight hash functions implement sponge constructions are SQUASH (6328 GE) GLUON (2071 GE), Quark (1379 GE), Photon (1120 GE) and Spongent.

The traditional key generation includes the generation of a key using the output of a random bit generator, the derivation of a key from another key, the derivation of a key from a password, and key agreement performed by two entities using an approved key- agreement scheme. NIST [SP 800-108] and [SP 800-133] standards recommend generation of cryptographic keys by direct or indirect use of approved Random Number Generator (RNG). The approved RNGs are specified in [SP 800-90], and [FIPS 186-4]. The cryptographic primitives for these approved RNG schemes consists of hash algorithms (SHA1, SHA2 or SHA3), generation of large primes, discrete logarithms from a large cyclic group etc. which are not suitable for implementing on low powered and low resourceful sensor nodes. Hence there is requirement for Light Weight Key Generation mechanism. NIST is in the final stage of drafting Light Weight Cryptographic (LWC) algorithms but still does not have any recommendations for light weight key generation or distribution mechanism.

As the IoT devices are outnumbering the devices on people's internet, much understood certificate issue process needs to be adapted for IoT devices too for identity management, key sharing etc. with approvals from authorized Certification Authority (CA) needs to be defined. Along with the process of issuance of certificates, the storage mechanisms of the key in constrained devices for IoT and the challenges for existing and future devices in compliance with X.509 needs to be seen.

The candidate algorithms for the proposed architecture short listed as per Fig.2 are described briefly further in this section.

1) CLEFIA

Literature survey shows that CLEFIA, a lightweight cipher developed by Sony Corporation and standardized by ISO/IEC 29192-2 in 2012, is a suitable candidate. CLEFIA is a 128-bit block cipher which supports key sizes of 128, 192 and 256-bits. CLEFIA uses i) Type-2 Feistel structure, suitable for efficient hardware implementation. ii) Diffusion Switching Mechanism (DSM) employed by the F-functions to obtain stronger immunity against differential and linear cryptanalyses. iii) Two different S-boxes based on different algebraic structures, which is expected to increase algebraic immunity. iv) Key scheduling algorithm using a generalized Feistel structure that facilitates easy analysis, to provide immunity against related-key attacks. Round keys and whitening keys are the two types used for encryption and decryption. The number of rounds of operation differs with the key size, 18 for 128bit, 22 for 192 bit and 26 for 256 bit keys.

The architecture proposed in [26] for CLEFIA accomplishes a high throughput of 592.58 Mbps and a low power consumption of 6.1 mW when synthesized using Semi-Conductor Laboratory (SCL) 180nm technology library. [27] works on the memory optimization of the CLEFIA to suit IoT applications.

2) PHOTON Hash

PHOTON uses a sponge-like construction and an AES-like to obtain a compact hash function. [28] evaluates the memory usage and latency of PHOTON on a Raspberry Pi 3 Model B. In [29], in order to improve the area-performance trade-offs of PHOTON hash function, an iterative architecture has been developed, which have been successfully synthesized, simulated and ported onto on several FPGA devices.

3) TRNG

A True Random Number Generator (TRNG) needs a nondeterministic source and used to seed the cryptographic algorithms. The non-deterministic sources are the unpredictable natural physical processes, like charging-discharging capacitors, voltage measured across resistors that are not driven, phase noise, etc. [30]. [31] discusses a robust, all-digital TRNG architecture that is built by adding de-correlation and de-biasing circuits to physical random number generators.

4) Authenticated Lightweight Key Exchange (ALIKE)

Authentication is one important component of security and privacy. The IoT vertical created a need to design and develop a lightweight secure authentication model, to provide immunity against attacks like Impersonation, man in the middle and unknown key sharing. Several Algorithms have been discussed, evaluated and compared in literature [32, 33].

5) Identity Based Signature

Lightweight authentication procedures using the unique IDs of IoT devices are proposed in [34]. This helps in providing identity - based encryption. [35] proposes a decentralized multi-signature protocol that combines Identity-Based

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

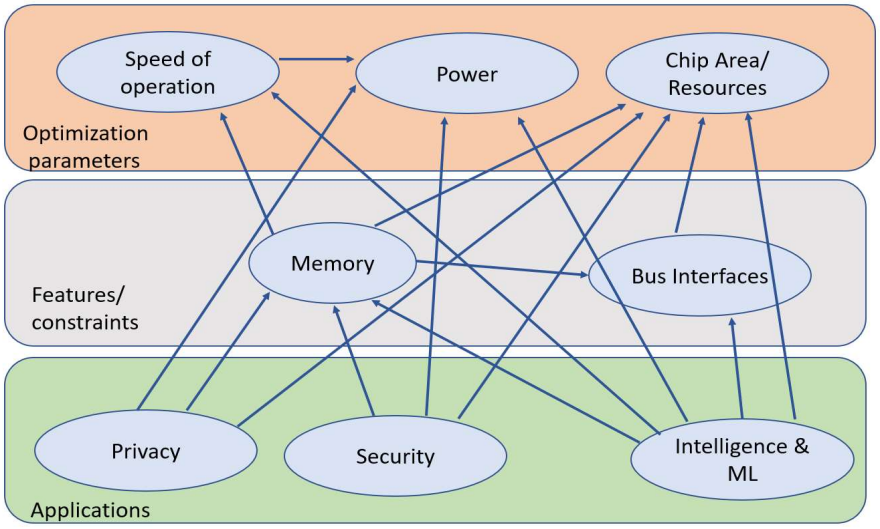

Fig. 3. Parameters and their interdependencies

Signature (IBS) with Schnorr scheme under discrete logarithms on elliptic curves.

6) CRYPTO-GPS

CRYPTO-GPS, is a well discussed Public Key Cryptographic protocol that has been considered for standardization in ISO/IEC 29192-4. It is focused towards asymmetric lightweight cryptography. The small area required for CRYPTO-GPS is attributed to regular addition and multiplication for integer computations. The results of a pre-computation are in the form of "coupons" [36, 37].

B. Homomorphic Encryption/Decryption Engine

The paradigm of cloud computing creates a threat to the privacy of data, especially in IoT verticals, wherein the personal data from homes and hospitals is now available at cloud servers. One of the solutions that can be applied to such scenarios is the usage of homomorphic encryption. Homomorphic encryption enables computations over encrypted data. This implies that the outsourced cloud services can perform computations on private data and provide the results without decrypting it. The types of computations and number of computations allowed on encrypted data depends on the type of homomorphic encryption, namely, partial, somewhat and fully homomorphic encryptions [38 and references therein]. Partial homomorphic encryption supports either addition or multiplication. Somewhat HE supports both addition and multiplication, but only to perform limited operations. FHE allows the evaluation of arbitrary circuits of unbounded depth, and is the strongest of homomorphic encryption [39]. [40] describes the design of Hardware Architecture for Fully Homomorphic Encryption (FHE) Algorithms in FPGA. The FPGA implementation of the Learning with Errors (LWE)-based FHE algorithm is demonstrated.

Using all these algorithms as part of System on chip (SoC), The proposal in this paper is to achieve security and privacy as described in this section.

V. CHALLENGES IN DEVELOPMENT OF OF PROPOSED SOC

Power, Performance, and chip Area (PPA), historically have been the three parameters of optimization in semiconductor designs. Cost as function of performance and area were the parameters of consideration in the older designs. The mobiles with battery backed power, however, diverted the optimization problem towards minimal power consumption. The trend with IoT devices is the extra requirements of security and privacy. Edge IoT devices, additionally have the analytics and ML requirements. The constraints are on the memory and the bus interfaces used. Fig.3 shows the parameters and their inter-dependencies, which makes the design of SoC for ethical and secure edge IoT challenging.

A. Approach

Integration of modules with the core, and the integrated performance testing and evaluation, are performed after unit level testing and evaluation. Identification or design, evaluation and integration of i) Light weight crypto algorithms for low power security implementation, general IO interface for interfacing high data sensors, ii) Homomorphic encryption library for low power microcontrollers, iii) analysis of optimum memory requirement for reduced die area, iv) Open source uDMA, AMBA APB/AHB, AXI cores for integration, v) Cache core and FIFO cores for optimization, vi) Identification of MPPT controller for optimization, are the stage-wise design choices that need to be made. Integrating each block and running simulations for identifying the functional issues along with achieving performance of the whole design, within the constraints of memory and bus interfaces, is a real challenge.

C. Implementation & evalution

In the case of FPGA implementation, it is important to understand the design and architecture of the targeted FPGA, before analyzing the evaluation report. Subsequently, the various optimization flags in the compiler need to be

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

experimented to get the best performance speed for minimal resources and power. The optimization flags can Kernels, disable, modify the handshaking protocols, etc.[41, 42].

The analysis of high-performance IO blocks has been carried out to verify the high speed IO functionality required for the high end IoT edge SoC, similarly Carry8 block analysis will help in integrating the CNN accelerator as part of the FPGA that is being used for prototyping the envisaged complex design. Analysis of Global clock buffers was done to make sure that enough clock buffers are available in the FPGA for implementing the complete RISC-V enabled ethical intelligent IoT Edge.

The complete cryptographic block using light weight standard compliant crypto algorithms will be implemented from scratch and these blocks gets integrated with remaining blocks of SoC for providing required adequate security for the IoT EDGE devices. The algorithms that are being planned for implementation are CLEFIA for Symmetric Key Cryptography, PHOTON for hash function, Authenticated light weight key exchange algorithm according to ISO 29192 standard. The implementation also includes TRNG, Digital Signature Algorithm.

Once proven on the FPGA, the design will be used to realize the SoC. The design flow optimizations for the SoC and the tools required need to be investigated further. In general design philosophy, the area occupied in the FPGA is 10 times more than a custom designed Application Specific Integrated Circuit (ASIC), and this metric will help us to understand the number of ASIC gates required for the selected RISC-V core. With respect to power consumption, FPGA designs are expected to consume 10 times more than the properly designed custom ASICs. The chip area occupied by ASIC is 10 times lesser than the area occupied in FPGA while implementing any complex design.

VI. CONCLUSIONS

Open-source RISC V cores have been shortlisted and the power, performance and resource analysis have been conducted. It has been seen that PicoRV32 consumes resources, relatively lesser than Roa Logic, with a performance upto 200MHz, thus seeming the best candidate for further development. The challenges involved in the development of SoC for Edge in IoT domain have been discussed. An architecture supporting security and privacy has been presented. The further approach that will be taken to realize the SoC has been discussed.

ACKNOWLEDGEMENT

The authors are thankful to the Electronics, IT & BT Government of Karnataka for supporting this work under the CIET project.

REFERENCES

[1]. S. Naveen and M. R. Kounte, "Key Technologies and challenges in IoT Edge Computing," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 61-65, doi: 10.1109/I-SMAC47947.2019.9032541.ConferenceName:ACM Woodstock conference

[2]. N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob and M. Imran, "The Role of Edge Computing in Internet of Things," in IEEE Communications Magazine, vol. 56, no. 11, pp. 110-115, November 2018, doi: 10.1109/MCOM.2018.1700906.

[3]. A. Adel et al., "Implementation and Functional Verification of RISC-V Core for Secure IoT Applications," 2021 International Conference on Microelectronics (ICM), 2021, pp. 254-257, doi: 10.1109/ICM52667.2021.9664926.

[4]. Samuel K. Moore, RISC-V AI Chips Will Be Everywhere IEEE Communication magazine, 24 FEB 2022

[5]. P. D. Schiavone et al., "Arnold: An eFPGA-Augmented RISC-V SoC for Flexible and Low-Power IoT End Nodes," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 4, pp. 677-690, April 2021, doi: 10.1109/TVLSI.2021.3058162.

[6]. R. Serrano et al., "A Low-Power Low-Area SoC based in RISC-V Processor for IoT Applications," 2021 18th International SoC Design Conference (ISOCC), 2021, pp. 375-376, doi: 10.1109/ISOCC53507.2021.9613880.

[7]. M. Sarmiento et al., "Systems on a Chip with 8bits and 32bits Processors in 0.18µm Technology for IoT Applications," in IEEE Transactions on Circuits and Systems II: Express Briefs, doi: 10.1109/TCSII.2022.3161494.

[8]. M. O. Demirtürk and B. Örs, "Low Energy Consuming SoC Design for IoT Applications," 2019 11th International Conference on Electrical and Electronics Engineering (ELECO), 2019, pp. 479-483, doi: 10.23919/ELECO47770.2019.8990635.

[9]. M. Urbina, T. Acosta, J. Lázaro, A. Astarloa and U. Bidarte, "Smart Sensor: SoC Architecture for the Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6567-6577, Aug. 2019, doi: 10.1109/JIOT.2019.2908264.

[10]. E. Flamand et al., "GAP-8: A RISC-V SoC for AI at the Edge of the IoT," 2018 IEEE 29th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2018, pp. 1-4, doi: 10.1109/ASAP.2018.8445101.

[11]. Z. Zang, Y. Liu and R. C. C. Cheung, "Reconfigurable RISC-V Secure Processor And SoC Integration," *2019 IEEE International Conference on Industrial Technology (ICIT)*, 2019, pp. 827-832, doi: 10.1109/ICIT.2019.8755206.

[12]. Guard Kanda and Kwanki Ryoo (2022), Design of an Integrated Cryptographic SoC Architecture for Resource-Constrained Devices. IJEER 10(2), 230-244. DOI: 10.37391/IJEER.100231.

[13]. R. Krishnamoorthy *et al*., "Systematic Approach for State-of-the-Art Architectures and System-on-Chip Selection for Heterogeneous IoT Applications," in *IEEE Access*, vol. 9, pp. 25594-25622, 2021, doi: 10.1109/ACCESS.2021.3055650.

[14]. D. A. N. Gookyi and K. Ryoo, "Selecting a Synthesizable RISC-V Processor Core for Low-cost Hardware Devices," Journal of Information Processing Systems, vol. 15, no. 6, pp. 1406-1421, 2019. DOI: 10.3745/JIPS.03.0129.

[15]. [Repository], Roa Logic, 2018 (Online). Available:,https://github.com/RoaLogic/RV12/blob/master/docs/RoaLogic_RV12_RISCV_Datasheet.pdf,[Last Accessed on 05.12.2022]

[16]. V. Melikyan, E. Babayan, A. Melikyan, D. Babayan, P. Petrosyan, E. Mkrtchyan, "Clock gating and multi-VTH power design methods based on 32/28 nm ORCA processor," in Proceedings of IEEE East-West Design and Test Symposium (EWDTS), Batumi, Georgia, 2015; pp. 1-4.

[17]. [website], SiFive, 2016 (Online). Available:,https://static.dev.sifive.com/E31-Coreplex.pdf, [Last Accessed on 05.12.2022]

[18]. [Repository], Syntacore, 2019 (Online). Available:,https://github.com/syntacore/scr1/blob/master/docs/scr1_eas.pdf, [Last Accessed on 05.12.2022]

[19]. [website], K. Asanovic, R. Avizienis, J. Bachrach, S. Beamer, C. Celio, H. Cook, et al., 2016 (Online). Available:,https://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-17.pdf, [Last Accessed on 05.12.2022]

[20]. [website], C. Celio, P. F. Chiu, B. Nikolic, D. A. Patterson, and K. Asanovic, 2017 (Online). Available:,https://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-157.pdf, [Last Accessed on 05.12.2022]

[21]. C. Duran, L. Rueda, G. Castillo, A. Agudelo, C. Rojas, L. Chaparro, H. Hurtado, et al., "A 32-bit RISC-V AXI4-lite bus-based

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.

microcontroller with 10-bit SAR ADC," in Proceedings of 7th IEEE LatAmerican Symposium on Circuits and Systems (LASCAS), Florianopolis, Brazil, 2016;pp. 315-318.
[22]. [Repository],C. Wolf, (Online). Available:,https://github.com/cliffordwolf/picorv32, [Last Accessed on 05.12.2022]
[23]. N. Gala, A. Menon, R. Bodduna, G. S. Madhusudan, V. Kamakoti, "SHAKTI processors: an open-source hardware initiative," in Proceedings of 29th IEEE International Conference on VLSI Design and 15th IEEE International Conference on Embedded Systems (VLSID), Kolkata, India, 2016;pp. 7-8.
[24]. [Repository], B. Hu, (Online). Available:,https://github.com/SI-RISCV/e200_opensource/blob/master/doc.[Last Accessed on 05.12.2022]
[25]. ISO, ISO/IEC 29192-2:2019, Information Technology - Security Techniques - Lightweight Cryptography, Available at: https://www.iso.org/standard/78477.html, [Last accessed on 17th March, 2023]
[26]. P. Saravanan, S. S. Rani, S. S. Rekha and H. S. Jatana, "An Efficient ASIC Implementation of CLEFIA Encryption/Decryption Algorithm With Novel S-Box Architectures," 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP), Chennai, India, 2019, pp. 1-6, doi: 10.1109/ICESIP46348.2019.8938329.
[27]. K. D. Muthavhine and M. Sumbwanyambe, "Conversion of Clefia Algorithm to Decrease Memory Restrictions Encountered on IoT by Applying CMA Method," *2022 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, Durban, South Africa, 2022, pp. 1-9, doi: 10.1109/icABCD54961.2022.9856353
[28]. T. Mangole, A. S. J. Helberg and K. K. Nair, "Resource Usage Evaluation of the PHOTON Hash Function," in *Conference on Information Communications Technology and Society (ICTAS)*, Durban, South Africa, 2022, pp. 1-6, doi: 10.1109/ICTAS53252.2022.9744686.
[29]. M. O. A. Al-Shatari, F. A. Hussin, A. A. Aziz, G. Witjaksono and X. -T. Tran, "FPGA-Based Lightweight Hardware Architecture of the PHOTON Hash Function for IoT Edge Devices," in *IEEE Access*, vol. 8, pp. 207610-207618, 2020, doi: 10.1109/ACCESS.2020.3038219.
[30]. S. Taneja and M. Alioto, "Fully Synthesizable Unified True Random Number Generator and Cryptographic Core," in *IEEE Journal of Solid-State Circuits*, vol. 56, no. 10, pp. 3049-3061, Oct. 2021, doi: 10.1109/JSSC.2021.3090247.
[31]. V. R. Pamula, X. Sun, S. Kim, F. u. Rahman, B. Zhang and V. S. Sathe, "An All-Digital True-Random-Number Generator with Integrated De-correlation and Bias Correction at 3.2-to-86 MB/S, 2.58 PJ/Bit in 65-NM CMOS," in *IEEE Symposium on VLSI Circuits*, Honolulu, HI, USA, 2018, pp. 1-2, doi: 10.1109/VLSIC.2018.8502375.
[32]. O. Catrina and S. -I. Stanciu, "Comparative Performance Evaluation of Key Exchange Protocols," in*14th International Conference on Communications (COMM)*, Bucharest, Romania, 2022, pp. 1-6, doi: 10.1109/COMM54429.2022.9817281.
[33]. M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," in *20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon, Korea (South), 2018, pp. 481-487, doi: 10.23919/ICACT.2018.8323802.
[34]. B. B. Gupta, A. Gaurav, K. T. Chui and C. -H. Hsu, "Identity-Based Authentication Technique for IoT Devices," in *IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2022, pp. 1-4, doi: 10.1109/ICCE53296.2022.9730173.
[35]. H. Liu, D. Han, M. Cui, K. -C. Li, A. Souri and M. Shojafar, "IdenMultiSig: Identity-Based Decentralized Multi-Signature in Internet of Things," in *IEEE Transactions on Computational Social Systems*, doi: 10.1109/TCSS.2022.3232173.
[36].] Dong, Qingkuan & Ding, Wenxiu & Wei, Lili, "Improvement and optimized implementation of cryptoGPS protocol for low-cost radio-frequency identification authentication," in *Security and Communication Networks*, 8. 10.1002/sec.1096.
[37]. Canard, S., Ferreira, L., Robshaw, M., "Improved (and Practical) Public-Key Authentication for UHF RFID Tags," in: Mangard, S. (eds) *Smart Card Research and Advanced Applications*. CARDIS 2012. Lecture Notes in Computer Science, vol 7771. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37288-9_4
[38]. Alexander Wood et.al., "Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics," in *ACM Computing Surveys*, August 2020 Article No.: 70 https://doi.org/10.1145/3394658
[39]. Fursan Thabit, Ozgu Can, Sharaf Alhomdy, Ghaleb H. Al-Gaphari, Sudhir Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing,"in *International Journal of Intelligent Networks*, Volume 3, 2022, Pages 16-30, ISSN 2666-6030, https://doi.org/10.1016/j.ijin.2022.04.001.
[40]. S. Behera and J. R. Prathuri, "Design of Novel Hardware Architecture for Fully Homomorphic Encryption Algorithms in FPGA for Real-Time Data in Cloud Computing," in *IEEE Access*, vol. 10, pp. 131406-131418, 2022, doi: 10.1109/ACCESS.2022.3229892.
[41]. [website], Xilinx, 2016 (Online). Available:https://www.xilinx.com/support/documentation/ip_documentation/lmb_v10/v3_0/pg113-lmb-v10.pdf, [Last Accessed on 05.12.2022]
[42]. [website] [manual], Xilinx, https://docs.xilinx.com/r/en-US/ug1400-vitis-embedded/Specifying-Debug-and-Optimization-Compiler-Flags, [Last Accessed on 05.12.2022]

Authorized licensed use limited to: International Institute of Information Technology Bangalore. Downloaded on July 01,2024 at 05:34:57 UTC from IEEE Xplore. Restrictions apply.