SIE 2015
6th International Symposium on Industrial Engineering
24th-25th September 2015
FACULTY OF MECHANICAL ENGINEERING
STEINBEIS ADVANCED RISK TECHNOLOGIES
INNOVATION CENTER FME

PROCESSOR SYSTEM ARCHITECTURES AND SECURITY

Zlatko Langović[1], Brankica Pažun[2], Duško Tomić[3]
[1]Faculty for Business Studies, Megatrend University, Serbia
[2,3]Faculty of Engineering Management, Alpha University, Serbia

Abstract. *There has been intensive development in telecommunications, financial services, industrial complexes. The system development is enabled due to hardware and software, as well as cloud computing and mobile systems development and data center. The importance of processor is huge because these devices i.e. computer systems represent the base for developing all layers of a modern information system. Future trends in processors developing are defined in the form of an improvement of CISC and RISC concepts and their synthesis into SoC platform. Security technologies implemented in processors- enable better security functions in information systems. This paper presents development of security technologies and processor architectures, and their impact on business information system.*

Key words: *AES, ARM TrustZone, HSA, x86*

1.INTRODUCTION

CISC and RISC architecture concepts represent a challenge for companies engaged production and development of processor technology. These concepts appear in the form of X86 and ARM architecture.

New solutions developing is defined through integration in the form of multiple cores on the same platform, SoC systems. In a given SoC platforms are implemented HSA (Heterogeneous System Architecture), GCN (Graphics Core Next Architecture) and CUDA (Compute Unified Device Architecture) subsystems that generate stronger processor architectures.

Due to achieving information system full potential, ther is necessity of existing high-quality security and energy efficiency.

Security technologies implemented in processors of major companies are: Intel TXT and Intel AES-NI, Intel Virtualization Technology (Intel VT), Trusted Execution Environment (TEE) and ARM TrustZone features.

2.TRADITIONAL PROCESSOR ARCHITECTURES – CISC AND RISC

According to the second quarter server shipments, Gartner figures for 2014, the revenue from x86 servers grew by 12.7% in Europe [4].

Intel-represents the idea about implementation of traditional x86 and achieving low power consumption with optimal capabilities sustention.

Intel has introduced line of Intel Xeon processor products D [5], which brings Intel's first system-on-chip (SoC) based on the Intel Xeon processor. Multi-core processor is implemented in the form of a SoC (System-on-chip SoC).

The line of products Intel Xeon processor D is based on the latest Intel 14-nanometer technology. Characteristics of SoC systems are small dimensions and low energy consumption.

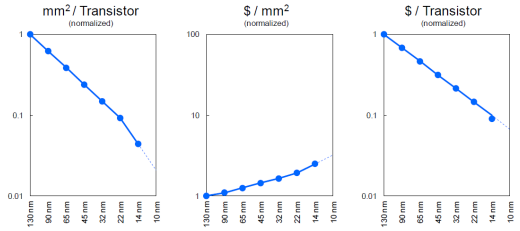

Fig.1. Cost per Transistor (Source: http://www.intel.com)

New Intel Pentium M [5] chip with a new 14-nanometer technology i.e. x86 processor, has better performance and lower energy consumption. Application of Intel M processor could be seen in cloud computing, IoT (Internet of Things), personal computers and mobile devices.

Zen, the name of the new high-performance processors, belongs to AMD. [7] This processor has one cluster for integers processing. Processor allows "deeper" pipelining and stronger effect during single-threaded tasks execution. Increased number of kernels improves parallelization process properties.

Due to AMD data, given processor has two 256bit units that enable better execution of 512b's tasks with numbers with floating point. These characteristics allow execution of relatively simple tasks in smaller intervals.

Optimal use of RISC system is now in data centers and mobile systems.

The phenomenon that is increasingly present in the business environment is IoT which generates a large amount of data that need to be preserved. This need for keeping data foregrounds data centers.

IoT market, including hardware, software, services and security, will increase from $1.3 trillion in 2013 to $3 billion in 2020, IDC predicts by 2018, 40% of the IoT-created data will be stored, manage and analyze near, or on the brink of a network. [8]

Processors with ARM architecture enter the market of server machines.

Samsung as processor manufacturer, uses ARM matrix. Processor is made in 14-nanometer technology. Unlike its predecessor, the processor 22 or 20 nanometer technology, the new processor has smaller dimensions and greater efficiency. [10]

Market analysts expect the ARM processors share of 20% of server shipments by 2019. [9]

3.CONTEMPORARY PROCESSOR ARCHITECTURES

New processor solutions appear in merging form of CPU and GPU on a single chip so-called SoC system. AMD has started applying this concept in Fusion processors line [6], while Intel has implemented given graphics resources in line Westmere, Sandy Bridge, etc. [5]

The main advantages of this integration is simplicity and graphical resources availability (for server machine) without adding graphics devices, which increase consumption.

This configuration can support desktop virtualization, perform redering video material without environment help. This group includes two processors: Xeon E3 [5] and AMD Opteron X. [6]

Given integration could improve graphics functions to some extent, toward low energy consumption and financial investment. GPU isolated on the graphics card does not overload computer resources, but investments are higher, with increase in energy consumption.

AMD has developed an architecture HSA (Heterogeneous System Architecture) [12], which allows developers to address "any" processing unit, and do not have to write separate sets of instructions, for CPU and for graphics subsystem. For example, different sections of the processor hardware (mostly CPU, GPU) are able to address shared memory.

HSA Foundation defines development and standardization process. This organization develops software tools at the API low level due to more productive implementation of mentioned concept. API is defined by HSAIL (HSA Intermediate Language), which allows developers writing code in appropriate higher-level programming language. Compiler translates code into HSAIL, while HSA working environment generates corresponding binary code.

AMD has developed a range of tools ie. development libraries and APIs, with the purpose to provide HSA utilization in Java, C++, OpenCL, C++ AMP, C#, OpenMP and Python, according to optimal hardware resources usage and energy savings. [16]

Nvidia CUDA (Compute Unified Device Architecture) technology presents a similar technology. Given system includes PTX function (Parallel Thread Execution). [7]

CUDA performs only on Nvidia graphics cards, while HSA belongs to open technology claster.

There has to be mentioned attemptation of two systems CISC and RISC processors integration on a single chip, defined in Skybridge project [6] [13]. This project was officially abolished recently [14].

AMD solution, Skybridge, allowed integration of technology HSA with ARM core and X86 core on the same platform (SoC system). Two chips use compatible interface that enables common memory controller usage, PCIe interface, the cache structure, with implemented HSA system, with the same I/O standards.

AMD has presented Carrizo, the new AMD APU. Improving could be seen in new x86 Excavator processor cores combined with GCN (Graphics Core Next Architecture) GPU. HSA technology has been integrated in the chip. Given subsystem combination

enables better product performance. This is the first AMD SoC processor designed for mobile PC market. [6]

AMD announced the new APU product that includes Zen core and graphics unit, codenamed Greenlend. It is assumed that this APU would own HBM (High Bandwidth the Memory) subsystem, as well. This platform has four channel DDR4 and PCI 3.0. Support for DDR4 has ECC with speeds up to 3200 MHz, with total capacity of 256 GB per channel. Each core has 512KB L2 cache. Each cluster of four Zen cores share 8MB L 3keša. Graphics performance are up to 16 GB HBM memory and flow about 512 MB s. Given chip can consist of 16 Zen cores, while server version can have 32 cores. [15]

4.PROCESSOR SYSTEM SECURITY

Security companies have become particularly important in today's development of ICT technologies, ie. Cloud technology, Open Daylight, NFV, SDN, etc.

Stuxnet is malicious software discovered in 2010 and designed to attack the PLC (programmable logic controllers industrial) systems [17] [18].

Today data is transfered through an unknown cloud system, and mobile device users move out outside of the secured corporate space, etc. Data movement in this environment creates necessity for higher quality security levels. Intel creates new products with improved security for potential users. Intel's solution are: Intel Xeon processor E5 family and Intel Xeon E7, providing new levels of hardware security capabilities. Due to enhance security at the company level as well as in Cloud systems, Intel has developed a number of options.

Intel Platform System Protection Technology with Intel Trusted Execution Technology (Intel TXT) defines software component integrity that is hardware based. This system enables increased safety in virtualized workload managing.

Function Intel Data Protection Technology with Intel Advanced Encryption Standard New Instructions (Intel AES-NI) strengthens data protection. Intel AES-NI enables secure transfer through decryption. Intel Data Protection Technology with Intel Secure Key provides additional data protection due to creating high-quality keys for cryptographic protocols.

Intel Virtualization Technology (Intel VT) increases security of hardware-based Cloud infrastructure through isolation of virtualized workload. [5]

Advanced security features implemented in Intel TXT and Intel AES-NI improve information system security, as well as Cloud structure safety.

Smart phones and tablets provide large set of services for consumers. To realize their full potential, mobile devices require not only energy efficiency and performance, but safety as well.

ARM operates with its partners and standardization organizations due to simplier and faster platforms and devices development with security features based on TrustZone technology. As a part of this initiative, ARM has created TrustZone Ready Program, designed to simplify the development of chipsets and devices with hardware-supported system Trusted Execution Environment (TEE). [11]

ARM technology is built into millions of smartcards and SIM devices. Central components of given devices are the SecurCore subsystems which allow flexibility and traditional microcontrollers programming.

Strong protection has a family of Cortex-M processors. This system provides cryptographic protection, security, storage and professional entropy sources, such as random number generators, partners are already enabling a secure Internet of Things.

AMD generates a dedicated AMD secure processor implemented in the corresponding AMD Accelerated Processing Units (APU). ARM TrustZone, technology with system approach, operates at higher hardware layers, creating safe environment and sharing the CPU setting to two virtual “worlds”. this response tasks are active in the "secure world" standard operations are active in the area "Normal World." Given technology ensures the security of sensitive data, that is, applications. With this system provider services, ie. business system key resources are protected. [6] [19]

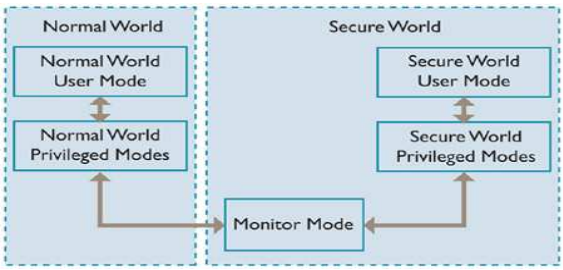

Fig.2. TrustZone (Source: http://www.anandtech.com/show/6007/amd-2013-apus-to-include-arm-cortexa5-processor-for-trustzone-capabilities

5.CONCLUSION

Processor system development takes place in several directions. Traditional architectures continue to live in the form of x86 and ARM concepts. Leading companies develop given systems in sence of better performance, energy consumption and security features. The 14-nm technology is commercialized with tendency of decreasing value in the future. ARM enters the server machine market, while x86 in the field of mobile systems. The new approach performs existing concepts' synthesis into a heterogeneous system, as SoC platform. Given platforms require new HSA, CUD and CNG architectures, which enable system managing at higher programming level. Security processing functions fulfill security services of various business systems, for example, banking systems and telecommunication companies, industrial complexes, etc. They reduce system complexity and energy consumption, as well. Development of processor architecture ie. security functions enables information system development. Further, information system development leads to business system development, characterised by less costs and higher productivity and efficiency.

REFERENCES

[1] Langovic, Z., Pazun, B., Tomasevic, V.: Impact of IS network virtualisation (SDN) on business improvement, International Conference, SMEs development and Innovation: Building competitive future of South-Eastern Europe, Ohrid, Macedonia, 2014

[2] Langović, Z., Milićević, A., Pažun, B.: Impact of processor technology on business system, International Quality Conference, Faculty of Engineering, University of Kragujevac, 2015

[3] Pažun, B., Langović, Z., Milićević, A.: integration of technologies OpenDaylight, OpenStack, NFV/SDN in business environment, International Quality Conference, Faculty of Engineering, University of Kragujevac, 2015

[4]Gartner company: http://www.gartner.com/technology/about.jsp (accessed 1.6.2015.)

[5]Intel company: http://www.intel.com/(accessed 1.6.2015.)

[6]Amd company: http://www.amd.com/ (accessed 16.6.2015.)

[7]Nvidia company: http://www.nvidia.com/ (accessed 10.6.2015.)

[8]http://searchnetworking.techtarget.com/news/2240242087/Intel-ARM-target-IoT-SoC-networking (accessed 15.6.2015.)

[9]http://www.computerweekly.com/news/2240226532/Arm-is-a-competitor-we-take-very-seriously-says-Intel (accessed 16.6.2015.)

[10]Samsung company: http://www.samsung.com/ (accessed 16.6.2015.)

[11]Arm company: http://www.arm.com/ (accessed 1.6.2015.)

[12]http://developer.amd.com/resources/heterogeneous-computing/what-is-heterogeneous-system-architecture-hsa/ (accessed 10.6.2015.)

[13]http://www.extremetech.com/computing/182790-amds-next-big-gamble-arm-and-x86-cores-working-side-by-side-on-the-same-chip (accessed 6.6.2015.)

[14]http://www.extremetech.com/computing/205078-amds-project-skybridge-the-armx86-hybrid-core-is-officially-dead (accessed 1.6.2015.)

[15]http://www.fudzilla.com/news/notebooks/37399-new-amd-zen-x86-apu-can-has-16-cores (accessed 6.6.2015.)

[16]http://www.hsafoundation.com/(accessed 6.6.2015.)

[17] http://www.reuters.com/article/2015/05/29/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 (accessed 15.6.2015.)

[18]http://www.theguardian.com/technology/stuxnet (accessed 1.6.2015.)

[19] http://www.anandtech.com/show/6007/amd-2013-apus-to-include-arm-cortexa5-processor-for-trustzone-capabilities (accessed 6.6.2015.)