European Cloud Processors

Motivation

Cloud processing is ubiquitous nowadays. Our digital society depends on millions of cloud processors sitting in datacenters processing data derived from all aspects of our daily activity: cloud processors handle all web transactions, which support ecommerce, news, entertainment, digital health, social networks, and personal communication. There are very few aspects of our daily life that are not mediated by a cloud processor. This trend, which started at the beginning of the century, is accelerating as novel areas are being engulfed by AI technologies that allow them to be processed in the cloud: driver assistance, video surveillance, environmental monitoring are now depending on the “cloud processing backbone”. While they use a lot of technology at the edge (i.e., inside the car, or in a remote sensing station), ultimately they are sending data to software applications running on top of a cloud processor inside a data center.

However, there are concerns about the security and sovereignty of data when it is stored on cloud processors located outside of Europe. To address these concerns, Europe needs to design its own cloud processor.

When data is stored on servers located outside of Europe, there is a risk that it could be subject to foreign laws and regulations, which could compromise the security and privacy of the data. By designing its own cloud processor, Europe can ensure that data is stored and processed within its own borders, under its own laws and regulations.

Furthermore, the use of cloud computing introduces new security risks, as data is transmitted over networks and stored on servers that may be vulnerable to cyberattacks. By designing its own cloud processor, Europe can implement security features that are tailored to its specific needs, and that take into account the unique threats that are faced by European businesses and organizations.

In the State of the Union Address in September 2020, President von der Leyen announced that “Europe should secure digital sovereignty with a common vision of the EU in 2030, based on clear goals and principles. The President put special emphasis on a ***European Cloud****, leadership in ethical artificial intelligence, a secure digital identity for all, and vastly improved data, supercomputer and connectivity infrastructures.”*

In a similar vein, Thierry Breton, EU’s Internal Market commissions indicated in September 2020: “*At the forefront of the major challenges is our* ***digital sovereignty****, which rests on three inseparable pillars: computing power, control over our data and secure connectivity. Firstly, Europe's* ***capacity to develop and produce the world's most powerful processors****, including quantum ones,* ***must be increased without further delay****. These microelectronic components underpin most of the key value chains of the future: cars and connected devices, tablets and smartphones, supercomputers and edge computers, artificial intelligence and defense.*” It is critical to produce a European cloud processor with the aim to have an all-EU solution that can be audited and shown to follow EU legislation in all its dimensions.

These goals can not be achieved without EU-based cloud processors that can follow the EU security, privacy and AI rules. Continuing to rely on non-EU hardware puts at risk basic guarantees for EU citizens that their data is truly processed according to EU legislation.

In addition, designing its own cloud processor can help Europe to promote innovation and economic growth. By developing its own cloud processor, Europe can create new opportunities for businesses and start-ups to develop innovative applications and services that are tailored to the needs of European customers. This can help to create new jobs and drive economic growth, while also ensuring that European businesses have access to the latest technologies and innovations.

Europe's Digital Decade emphasizes the importance of microprocessors: "*If connectivity is a precondition for digital transformation, microprocessors are at the start of most of the key, strategic value chains such as connected cars, phones, Internet of Things, high performance computers, edge computers and Artificial Intelligence. While Europe designs and manufactures high-end chips, there are important gaps, notably in state-of-the-art fabrication technologies and in chip design, exposing Europe to a number of vulnerabilities.*" This statement is right on point. Literally 0% of the high-end cloud processor solutions are designed in Europe, exposing the EU to a number of vulnerabilities.

Finally, designing its own cloud processor can help Europe to reduce its dependence on foreign technology providers. Currently, many European businesses and organizations rely on cloud infrastructure that is provided by large technology companies based outside of Europe. By designing its own cloud processor, Europe can reduce its reliance on these providers, and develop its own independent cloud infrastructure that is tailored to its specific needs.

Indeed, the **Digital Decade** also discusses the percentage of the EU market serviced by EU-made microchips: "*The position of European players is far below the EU's global economic weight in key technology areas like processors, web platforms and cloud infrastructure, for example 90% of the EU's data are managed by US companies, less than 4% of the top online platforms are European, European made microchips represent less than 10 % of the European market.*" A concerted effort needs to be made to counter this trend and increase the percentage of European made cloud processors.

In conclusion, there are many reasons why Europe needs to design its own cloud processor. By doing so, Europe can ensure data sovereignty, address security concerns, promote innovation and economic growth, and reduce its dependence on foreign technology providers. Ultimately, this will help to ensure that European businesses and organizations have access to the latest cloud technologies, while also protecting the security and privacy of European data.

Current Status

It is very simple to summarize the current status regarding the availability of European-made cloud processing technology: exactly **ZERO** European solutions exist today for cloud processing. Hence, supporting the design of a European Cloud processor is key to achieve the goals stated in the previous section.

There are three possible architectures to be used for a European-based cloud processor: x86, ARM or RISC-V.

The overwhelming majority of cloud processors are based on the x86 architecture, produced by two U.S.-based companies, Intel and AMD. However, as it is widely known, it is not possible to design x86 processors without special permission from Intel. Hence, x86 is not an option for the EU.

A second avenue could be to produce a cloud processor based on the licensable ARM architecture, controlled by Softbank, a Japanese entity. There have been many attempts by companies licensing the ARM architecture to enter the cloud market, with limited success so far (Applied Micro, Ampere, Marvell, Qualcomm). Probably the most successful ARM solution currently is the one deployed by Amazon AWS yet, still, it's a U.S. based design. However, the business future of the ARM architecture is unclear, and certainly not controlled by the EU. There was a purchasing attempt by Nvidia, stopped by regulators. Its current owner, Sofbank, has expressed interest in divesting the ARM division through an IPO. It is unclear that the EU should base its long-term strategy in a proprietary architecture like ARM.

The best option for Europe is to base its future cloud computing processor on the open RISC-V architecture. RISC-V is an open standard defined by the RISC-V international foundation, an entity based in Switzerland. The RISC-V foundation makes its specification available to all, free-of-charge, and, very importantly, with the right to freely extend and modify the specification without restrictions. This makes RISC-V the right short-, medium- and long-term choice for Europe for its cloud infrastructure. The openness of the ISA allows multiple European players to supply competing designs. It protects customer, programmer and user investments by ensuring that, if a given European company disappears, another European RISC-V player can take its place, without requiring costly re-programming of applications and middleware.

Research Challenges

Cloud processors have special characteristics making them different from laptop processors or from HPC processors used in supercomputers. They are tailored to both the needs of cloud software as well as reflect the fact they are used in very large aggregations within a data center. Furthermore, they have a special emphasis on data security and privacy, as they are concurrently running applications that contain private data from different (non-mutually trusting) users.

Cloud processors are designed to handle workloads in a cloud computing environment, where services and applications are hosted on remote servers and accessed over the internet. These processors are optimized for tasks such as running virtual machines, handling web requests, and processing large-scale data sets. They are typically designed to be energy-efficient and offer a balance of single-threaded and multi-threaded performance. Cloud processors may also have specialized features such as hardware acceleration for machine learning or high-speed interconnects for distributed computing. Cloud processors are also designed to handle a range of workloads, including virtualization, databases, and enterprise applications. These applications may require specialized features such as hardware acceleration for encryption or virtualization.

The challenges to be addressed to produce a European cloud processor are the following:

- Research, definition and design of a high-frequency, very wide (8-wide) out-of-order core, with the following key attributes
  - At least 3 memory operations issued per cycle
  - Native hardware support for virtual machines through a hypervisor layer

  - Extensive protection of processor internal storage through ECC
  - Support for cryptographic instructions
  - Support for security enclaves, either through separate memory spaces or a similar technology
  - Cache coherent
  - Support for efficient synchronization across cores
  - Support for multithreading
  - New forms of energy efficiency, energy allocation and energy rationing
  - Resistant to side-channel attacks
- Research, definition and design of a high-performance “uncore” tailored for the cloud, capable of
  - Supporting 16 to 128 of the above defined core
  - Supporting large second level and last level caches
  - Advanced prefetching techniques
  - Novel resource partitioning algorithms to split the hardware resources to different virtual machines following an administrator-set policy
  - Memory encryption techniques
  - Advanced network-on-chip
  - Advanced reliability techniques, for all “uncore” components
  - Energy and power controller techniques to manage the cores and the “uncore”
  - Secure boot technologies, preferably open-source, for maximum public scrutiny
  - High bandwidth off-ide interfaces, specially to remote memory (such as CXL memory)