TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Institute of Systems Architecture, Chair of Privacy and Data Security

Master Thesis

A secure e-health data processing platform using Confidential Computing

Manik Khurana

Born on: 2nd September 1998 in Dehradun, India
Matriculation number: 4991921
Matriculation year: 2020

20th September 2023

Supervisor
Dr. Ivan Gudymenko, Deutsche Telekom MMS

Supervising professor
Dr. Stefan Köpsell, TU Dresden

TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Datenschutz und Datensicherheit

AUFGABENSTELLUNG FÜR DIE MASTERARBEIT

Name, Vorname des Studenten:	Khurana, Manik
Immatrikulationsnummer:	4991921
Studiengang:	Distributed Systems Engineering

Thema (deutsch): **Sichere e-Health Plattform mittels Confidential Computing**

Thema (englisch): A secure e-health data processing platform using Confidential Computing.

Ziel:

With increasing data breaches and privacy concerns, it is now necessary to be sure about our data's security in the Cloud. Over this, we explore how the latest paradigm of Confidential Computing (CC) help in keeping the e-health records secure. A thorough technical survey of the available CC technologies, CC frameworks, legal requirements, and trust assumptions will be done. After the survey and implementation of these technologies, the top solutions as per the requirements will be presented and discussed in detail.

High-level tasks:

- A technical survey of available CC technologies, CC frameworks like SCONE, Fortranix, and their implementations.
- Compare the security and privacy implications and guarantees each framework provides.
- Implement and check for CC support along with the security & privacy guarantees in various CSPs like AWS, GCP, Azure, and OVHcloud thereby highlighting the differences.
- Derive the patterns for a dedicated platform supporting CC for e-health workloads.
- A concise analysis of legal requirements for e-health data processing on Cloud platforms mainly in European Union.
- Creation of Adversary model, explicit trust assumptions, and operational requirements based on the analysis of legal requirements.
- An evaluation use case will be taken from an existing e-health application and compared against.
- Provide a Secure Infrastructure-as-a-Service (IaaS) Cloud stack with support for CC.

Betreuer:	Dr.-Ing. Ivan Gudymenko (T-Systems MMS)
Verantwortlicher Hochschullehrer:	Dr.-Ing. Stefan Köpsell
Institut:	Systemarchitektur
Beginn am: 22.02.2023	Einzureichen am: 26.07.2023 (22 Wo)

22/2/23 Manik

Datum, Unterschrift der/des Studierenden

Unterschrift des betreuenden Hochschullehrers

Verteiler: Prüfungsamt (Original); Student (Original – Deckblatt der Masterarbeit); HSL + Sekr. (Kopie); elektr. Datei → Sekretariat

TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science Examination Office

Technische Universität Dresden, 01062 Dresden, Germany

Hr. Manik Khurana
Gutzkowstraße 29-33
Zimmer Nr. 410M
01069 Dresden

Distributed Systems Engineering – DSE

Contact: Dr. -Ing. Irina Karadschow
Telephone: +49 351 463-39613
Telefax: +49 351 463-38319
Email: infscis.dse@mailbox.tu-dresden.de

Dresden, 07.07.2023

Ihr Antrag auf Verlängerung vom 06.07.2023

Sehr geehrter Herr Khurana,

ihr Antrag auf Verlängerung der Masterarbeit wurde im Prüfungsausschuss behandelt.

Der Antrag wird teilweise abgelehnt.

Begründung:
Sie beantragten 12 Wochen Verlängerung.
Die Angaben von Gründen rechtfertigen dies nicht. Die Abwesenheit des Betreuers Ihrer Masterarbeit in der Firma stellt keinen Grund für die Verlängerung der Bearbeitungszeit dar.

Eine Verlängerung von acht Wochen kann Ihnen gewährt werden.

Das neue Abgabedatum entspricht nun dem 20. September 2023.

Rechtsbehelfsbelehrung: Gegen diesen Bescheid kann innerhalb eines Monats nach seiner Bekanntgabe schriftlich bei dem zuständigen Prüfungsausschuss, über das Prüfungsamt, Technische Universität Dresden, Fakultät Informatik-Prüfungsamt, 01062 Dresden oder zur Niederschrift über das Prüfungsamt, Technische Universität Dresden, Fakultät Informatik-Prüfungsamt, Andreas-Pfitzmann-Bau, Nöthnitzer Straße 46, 01187, Dresden Widerspruch eingelegt werden.

Mit freundlichen Grüßen

Prof. Horst Schirmeier
Prüfungsausschussvorsitzender

Statement of authorship

I hereby certify that I have authored this document entitled *A secure e-health data processing platform using Confidential Computing* independently and without undue assistance from third parties. No other than the resources and references indicated in this document have been used. I have marked both literal and accordingly adopted quotations as such. During the preparation of this document I was only supported by the following persons:

Dr. Ivan Gudymenko

Additional persons were not involved in the intellectual preparation of the present document. I am aware that violations of this declaration may lead to subsequent withdrawal of the academic degree.

Dresden, 20th September 2023

Manik Khurana

Abstract

Data privacy and its confidentiality have been a pertinent problem since the very start of Computation on the Cloud. Many technologies have been around for close to a decade now, and there is always a scope for improvement in all of them. Researchers have done enough to protect data at rest and data in transit. However, for data-in-use, which is the state of data while being processed, there are a few loopholes that can facilitate data leaks. In the case of e-health data and records of patient medical history, unauthorized access, and data breaches hurt the healthcare industry the most, and losing the data that are so important is a bad situation for the patient. In order to prevent it, this master thesis project proposes a solution for the SEMECO cluster. The solution is a Cloud stack (IaaS or managed) comprising various technologies under the Confidential Computing domain. Confidential computing is a cloud computing technology that isolates sensitive data in a protected CPU enclave during processing. This ensures vendor exclusion, meaning that even the CSP cannot access the data. A technical survey of available technologies along with their advantages, disadvantages, cost-to-pocket, security, privacy guarantees, etc. was done and compiled into graphs and charts. The technologies used to ensure this are - Intel SGX/AMD SEV, SCONE/Fortranix, Azure/AWS/GCP/OTC/OVH/Alibaba as CSP.

Keywords/Keyphrases: Confidential computing, data protection, security, healthcare.

Contents

List of Figures

List of Tables

1 Introduction

Problem

It is commonly known that data is becoming highly important for our modern economy. With time, more and more organizations are becoming a part of the Artificial Intelligence (AI) revolution while Cloud Computing has become a part of daily business. Information is constantly generated, consumed, shared, and stored. Computing systems are now more complicated than ever due to advancements in both hardware and software. The size and functionality of the software, particularly the most privileged kernel-level software, the one in charge of system security, have drastically expanded. For instance, the Linux kernel has increased from around 200k lines of code to around 22 million lines now. This evolution has made consolidation more possible than ever before, enabling systems to carry out more functions and complete more work with the same hardware. Many useful outcomes of this consolidation include the cloud and virtual data centers where anyone can purchase pocket-friendly computing time. However, both consolidation and complexity often have a negative impact on the security of a system.

With more and more data breaches happening around us, we must know our data's whereabouts. New studies show how big a market is for Data Loss/breaches. According to the IBM Report for 2022 [1], the healthcare industry's cost of data breaches has increased by 42 percent since 2020. For the 12th year in a row, in 2022, Healthcare has had the highest data breach cost of any industry with an average total cost of USD 10.10 million, which earlier was USD 9.23 million in 2021. Healthcare is considered one of the most critical infrastructures. When it comes to the platform, the report states that 45 percent (nearly half) of all data breaches, in all industries, happen in the cloud. The average cost of a data breach was around USD 4.35 million in 2022. Security Artificial Intelligence (AI) and automation did help reduce the loss but still cost companies an average of USD 3.05 million when their data was breached. Unauthorized access accounts for 19 percent of the total breaches which is almost 1/5th. In Germany, there was an average loss of USD 4.85 million in 2022 and USD 4.89 million in 2021 just due to Data Breach. With numbers this huge and the stakes this high, it's important to devise a new formula that can save companies from losing so much business, time, and money.

Another important issue is raised in the later sections where we introduce the readers to the OpenMRS - Medical Record System. The goal of this open-source project is to digitalize patient records to ensure quick retrieval, fairly secure storage, and the maintenance of patient medical history along with medicine prescriptions. The digital form of patient data and its metadata, further referred to as the e-health data is very important and hence needs to be secured to the best of our abilities from any insider/outsider observing/modifying attacks.

Task

This Master Thesis Project aims to survey the technical aspects of various cloud-based services and frameworks with respect to Security and Privacy. It also focuses mainly on storing and processing e-health data in a cloud environment that implements the superior Confidential Computing paradigm of platform and application security. In the previous section, it is highlighted how much money is wasted each year due to these data breaches, and this project is capable of contributing to saving a huge chunk of it when implemented. The legal laws of data storage and data processing in Germany and in the EU will also be studied during the research phase and the final product will have to adhere to these, in order for it to be selected. The final product in development will be pitched to the SEMECO cluster in Dresden, Germany. SEMECO stands for Secure Medical Microsystems and Communications. SEMECO aspires to transform existing approval procedures with innovative approaches to system solutions in order to increase the pace of innovation for intelligent medical equipment and implants. The emphasis is on an innovative mix of sensors, actuators, driving technology, and data processing. As part of the Clusters4Future initiative, a framework is being developed that capitalizes on the innovation and future potential of the electronic semiconductor and microsystems technology sectors for medical technology, coordinates legitimate regulatory and safety requirements, and develops market applications. The final product of the Thesis Project will be the top solutions which comprise the combinations of technology and services that could in itself, be a new IaaS Stack. For this, we intend to use the Confidential Computing paradigm for securing our e-health data on the already-secure cloud platform.

Overview

What is Confidential Computing?
There are already ways of protecting data via encryption at rest and Encryption in Transit. Confidential Computing adds to this a way that protects data even during its processing (Data in use) and how this can be verified. The Confidential Computing Consortium defined Confidential Computing (CC) as “the protection of data in use by performing the computation in a hardware-based, attested Trusted Execution Environment”, and identified three primary attributes that make a Trusted Execution Environment - data integrity, data confidentiality, and code integrity.

Why Confidential Computing?
It provides enhanced security of the system - it prevents breaches by keeping hackers, malware, and malicious insiders out of the system. And, it eliminates the need to trust the Cloud Service Provider as trust is the most important part of relying on it. It is compliant and offers new possibilities - complies with regulation and privacy expectations by analyzing data without looking at it which is great for e-health data. And, it creates data-driven business models that share data without actually sharing it.

One of the most secure ways people store their data is in paper form; for multimedia data there are on-premise hard disks. With that becoming a new task to deal with, the coming age of Cloud Computing technologies helps manage, orchestrate, and ease the process. Cloud computing is not just the storage provided online. It has three service models - IaaS, PaaS, and SaaS. The storage solution is mainly a SaaS application, which is some companies providing storage as a Service. It has four Deployment models - Public, Private, Community, and Hybrid. The well-known Cloud Service Providers including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) have their own security and privacy guar-

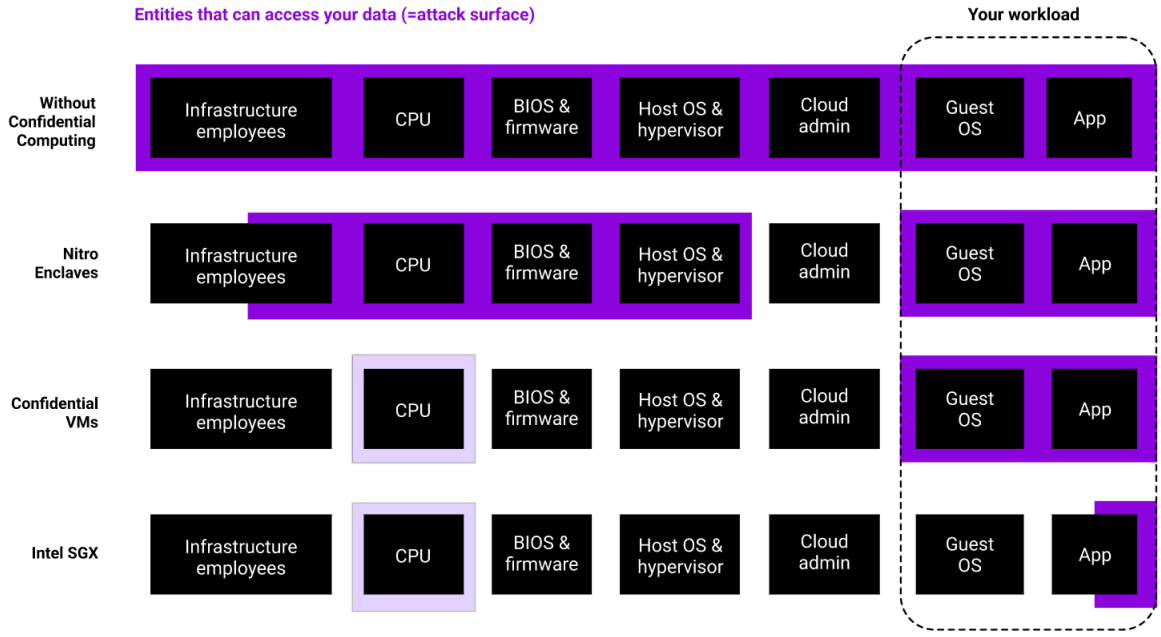

Figure 1.1: Reduced attack surface when compared to native system architecture [2].

antees. In the case of e-health data, it is more important than ever to be sure that the data will not be leaked or even accessed by anyone without authorization. Fig. 1.1 refers to the basic difference in the protected area of any system deployed Without Confidential Computing, on AWS Nitro Enclaves, on Confidential VMs, and with Intel SGX.

We move forward into Chapter 2 where you, the reader, will be introduced to various new technologies and systems that will help us achieve our goal of architecting a secure Confidential computing stack on a Cloud Service Provider. Chapter 3 lists the various offerings of Cloud Service Providers - AWS, GCP, Microsoft Azure, Alibaba Cloud, IBM Cloud, OVHCloud, and OTC. After getting to know the underlying technologies and their connection in the Cloud, in Chapter 4, we study the products and frameworks that are already in production. Some of them even have their own e-health offerings. In Chapter 5, we introduce the design principles kept in mind to build the final e-health Confidential Computing stack. This will give us the conclusion as to what we can imagine in our final stack, following which we implement the solution in Chapter 6. Chapter 7 refers to our observations when the implemented solution was assessed for its Security and Privacy readiness for our e-health scenario. The final Chapter 8 gives a short recap of the Thesis document and draws attention to why the selected choice is the best available choice for us at the moment.

2 Background

2.1 Confidential Computing (CC)

As detailed in the previous section, there are four additional attributes of Confidential Computing that may be present - code confidentiality, programmability, recoverability, and attestability. However, only attestability is strictly necessary for a computational environment to be classified as Confidential Computing [3]. When talking about data protection, it must be known that there are three states of Data - at rest, in transit, and in use. While there are well-known techniques to preserve data at rest and data in transit, the preservation of data in use and its verifiability while being processed are yet to be well known (Intel SGX and related). Data in-use refers to active data that is stored in a non-persistent digital state - in the system's random-access memory (RAM), CPU caches, or CPU registers.

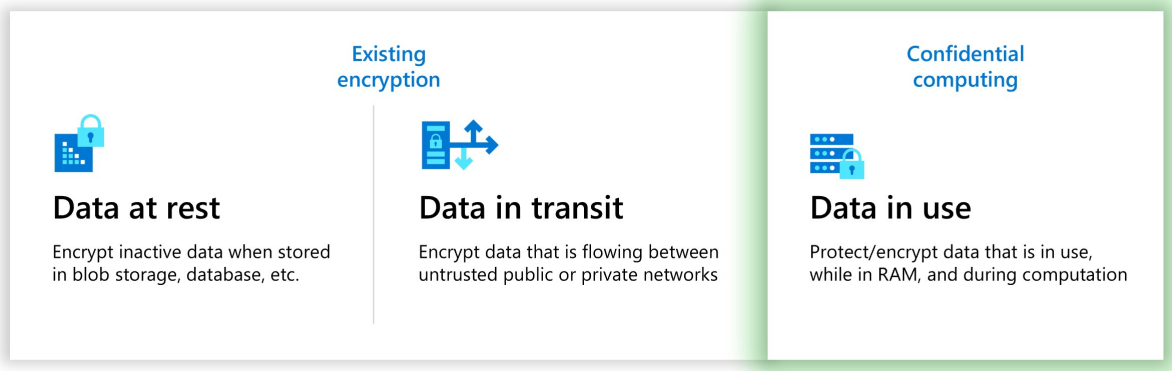

Figure 2.1: Data protection at three states - data-in-use for CC [4].

The three states of data as shown in Fig. 2.1 and its protection using:

- Encrypting files for storage or encrypting storage devices is an effective way to protect data stored in **at-rest** state.
- The **in-transit** state is the transfer of data between locations. To ensure the security of data in transit, users can encrypt files or utilize secure transmission protocols like HTTPS, Secure Sockets Layer (SSL), Transport Layer Security (TLS), and File Transfer Protocol with SSL Security (FTPS).
- Confidential computing was created to protect data **in-use** state.

In the Intel terminologies, Confidential computing is a stack of hardware and software that together work to address fundamental security issues of the cloud era, from edge security that supports federated learning and accelerated blockchain to data security in the public cloud. The trusted execution environment (TEE), also known as an **enclave**, is the foundation of that stack and is where data and code are isolated and protected from other software, such as the operating system and cloud service stack. Even with privileged root access, the code and data are protected against viewing and change from outside the TEE, thanks to the hardware protection of a section of the processor and memory that only approved code is allowed to execute on and access data on. This is achieved by physically encrypting a part of memory and altering memory access controls such that formerly privileged software (OS, hypervisor, etc.) can no longer access or see the data or application code within that enclave. Programs that make use of these enclaves can be created by developers using libraries and extensions like Intel SGX. Thus, the TEE offers the following four major advantages: A uniform development and deployment strategy; strong defense against both on-chip and off-chip unwanted accesses; no dependency on privileged software controlled by administrators; confirmation that the proper code is running on the right hardware [5].

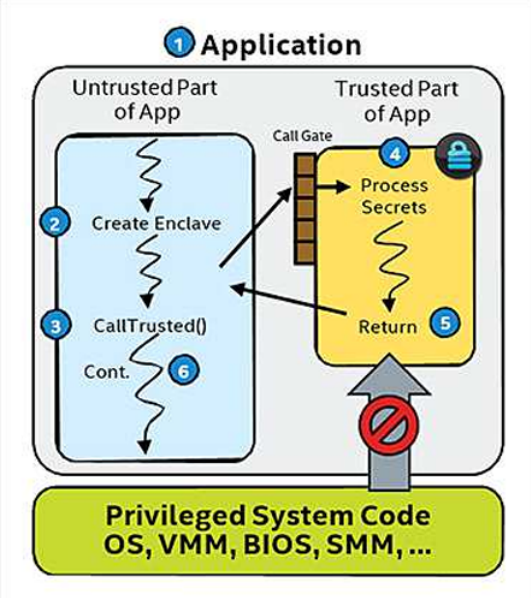

Figure 2.2: The separation of Trusted and Untrusted code in Intel SGX [6].

Fig. 2.2 illustrates the separation of the Untrusted and Trusted parts of the application and how the OS, VMM, etc. cannot access the trusted part of the application. Every application that is running establishes a unique protected area (the trusted enclave) with limited entry/exit locations specified by the developer. Only the code operating inside the enclave sees data in the clear (decrypted) when the trusted function is called. While enclave data sent to memory is encrypted and integrity checked, enclave code and data inside the CPU perimeter execute in the open. Enclave data is completely protected from outside access. The enclave data is still present in the trusted memory region after the function returns. As a result, there are guarantees that the data inside the enclave will stay private, unaltered, and more secure [5].

Confidential Computing Terminologies

Enclaves - Enclaves are available in many modern CPUs. These include but are not limited to, Intel SGX (2015), AMD SEV (2017), and Apple M1 (2020). They can also be created dynamically. They can run arbitrary programs. They have four defining security properties:

- **Isolation** - No one else CPU can look into the enclave. Not OS, no one.
- **Runtime memory-encryption**Runtime memory-encryption - Everything stored and processed inside the enclave is always encrypted in memory.
- **Sealing** - Allows to securely store state on an otherwise untrusted system.
- **Remote Attestation** - An enclave can convince a remote party that it is indeed a secure enclave and running on secure hardware. More on this in later sections.

All these four features combined are what can be understood as Confidential Computing. Technologies like Arm TrustZone, TPMs, and HSMs, often include 1-2 of these features (mainly isolation).

A confidential library is a library like an enclave that runs inside a hardware-based, certified TEE, isolated from other libraries of the same kind and any TEE hosting environment and allows usage by applications outside the TEE. A confidential process is a process like a Trusted Application that runs inside a hardware-based, attested TEE and is therefore isolated from other confidential processes and the TEE's hosting environment. A confidential container is an entry point process of a container image that is operated inside a hardware-based TEE with no access to any hosting environment or other confidential containers. A confidential VM is a Virtual Machine (VM) that runs inside a hardware-based, verified TEE, with the entire VM image being isolated from the host operating system and hypervisor, as well as from other private VMs and any hosting environment inside the TEE. Examples - AMD SEV, Intel TDX [7].

Use cases - Confidential Computing

In the Healthcare industry, these are the top confidential computing use cases [8] are:

- Protect data collected by platform operators and service providers.
- Assure partners and clients that you cannot view encrypted data.
- Stop platform software from gaining access to data.

2.2 Attestation

The system must continue to function reliably even with confidential computing [10]. It is important to demonstrate to the client that confidentiality and integrity of data are given top priority in the environment where their application is being used. To achieve this in a traditional scenario, they must start with a secure root of trust, a foundational component that is cryptographically secure. This typically takes the shape of a secure hardware module, like a Trusted Platform Module (TPM). TPM is the industry-accepted standard for secure, specialized cryptographic processing. It is a customized microcontroller that protects systems with a built-in set of cryptographic keys. Nevertheless, it is looking into a number of attestation mechanisms.

Because the CPU becomes a trusted entity in the majority of confidential computing implementations, the CPU (or a security processor linked to it) certifies that the contents of the VM and its encryption are configured correctly. It is usually not essential in this case to attest the hypervisor (or host operating system), which may not be trustworthy. In some cases, it may still be advised to use a fully certified environment to prevent replay attacks and potential CPU vulnerabilities. In these cases, they seek certification for the full hardware and software setup supporting the client's application. Attesting the underlying hardware,

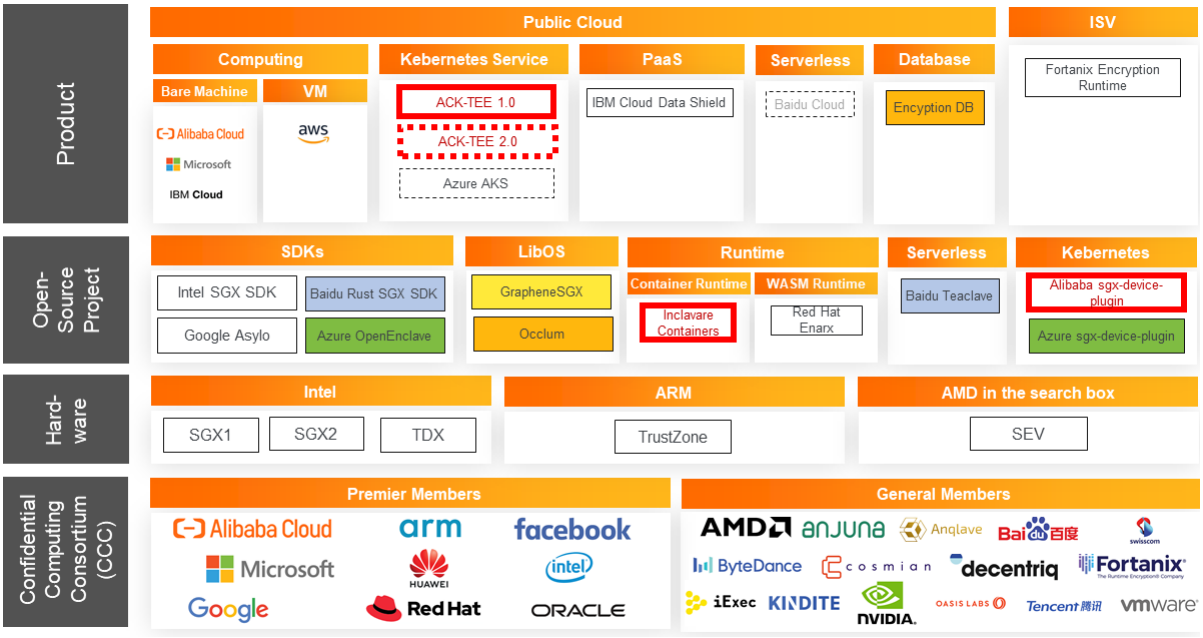

Figure 2.3: The Confidential computing Tech Industry in 2020 [9].

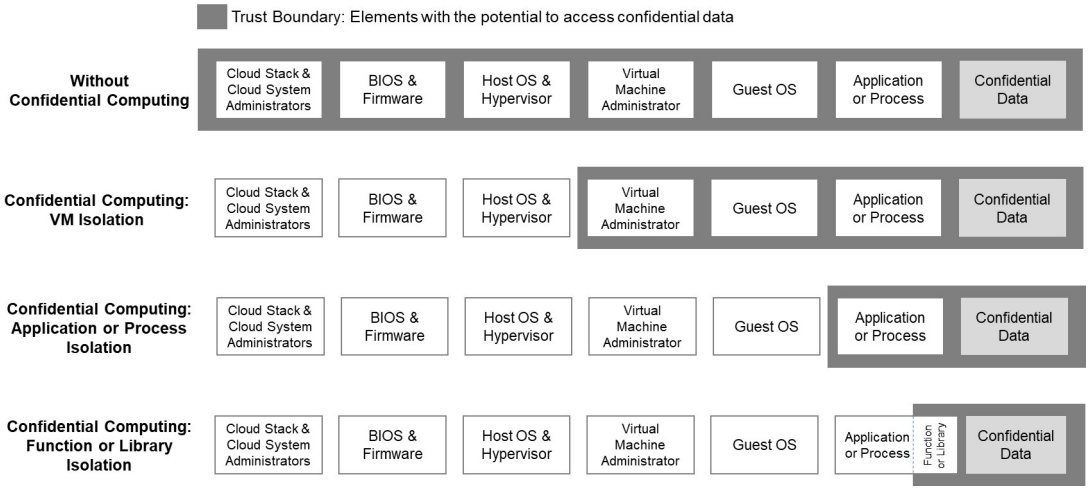

Figure 2.4: Confidential computing Trust Boundaries [8].

however, requires rethinking some of the fundamental parts of a processing system with a more intricate root of trust than a TPM in order to better attest the complete platform.

In comparison to solely cryptographic approaches (such as Fully Homomorphic Encryption (FHE) and Secure Multi-Party Computation), CC based on HW TEEs on commercial architectures has far higher confidence in hardware and software components. As a result, with Hardware TEEs, it is critical to ensure that the hardware is up to date with the most recent security features. TEEs do not give greater security assurances than traditional computing without attestation under the attacker models studied in CC. This is due to the fact that without attestation, a remote user cannot tell the difference between a malicious platform and a genuine one. This is true even for attestation alternatives such as authentication as defined in the recent paper from researchers at TU Dresden, Germany [12]. In the context of confidential computing, attestation is used to demonstrate the TEE's trustworthiness. It indicates which software layers are active on the TEE. The main constituents in the attestation procedure are as follows:

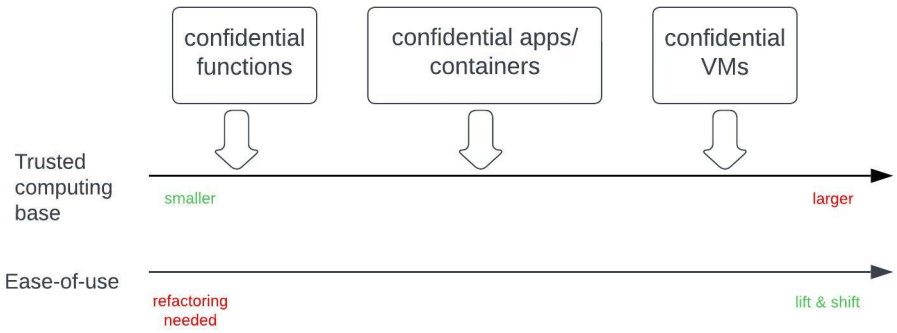

Figure 2.5: The Confidential Computing spectrum [11].

- **Attester** — The Attester is the entity that sends evidence to the relying party to tell them of the condition of the system. The evidence notifies the relying party on the system's status, the Trusted Computing Base (the trusted component of hardware, firmware, and software), and other features of the system. The evidence consists of a series of statements that are afterward stated or rejected by the verifier. The evidence is cryptographically authenticated using a key (often provided by the semiconductor manufacturer) that is utilized during the verification process.
- **Key Broker Service (KBS)/Relying Party** — The KBS is the reliant party, and its principal function is as follows:
  - The attester (confidential VM or container) provides evidence via the challenge-response protocol.
  - For verification, provide the evidence to the Attestation Service (Verifier).
  - Apply the assessment policy to the returned Attestation Results to determine the attester's credibility.
  - Interact with the Key Management Service to retrieve and send the keys to the attester.
- **Verifier (Attestation Service)** — The Attestation service evaluates evidence based on defined policies and reference values. Assume reference values to be "good" and "trusted" values which are established in advance time and used to validate the attester's proof. These reference values are frequently generated when the system firmware and software layers are being developed via a linked CI/CD workflow.
- A **Key Management Service** secures the storage, maintenance, and backup of cryptographic keys used by applications and users.

For our final product, it is essential we have Attestation capability. Confidential computing (CC) uses hardware-based Trusted Execution Environments (HW TEEs) on any of the commercial architectures and has much more trust in hardware and software components than purely cryptographic technologies (such as Fully Homomorphic Encryption or Secure Multi-Party Computation). As a result, with HW TEEs, it is critical to ensure that the hardware is updated with the most recent security features. TEEs do not give stronger security assurances than traditional computing without attestation under the adversarial models considered by CC. This is due to the fact that a remote user cannot tell the difference between a malicious platform and a genuine one without attestation. This is true even for attestation alternatives such as authentication. As a result, remote attestation is one of the important features of a TEE [14].

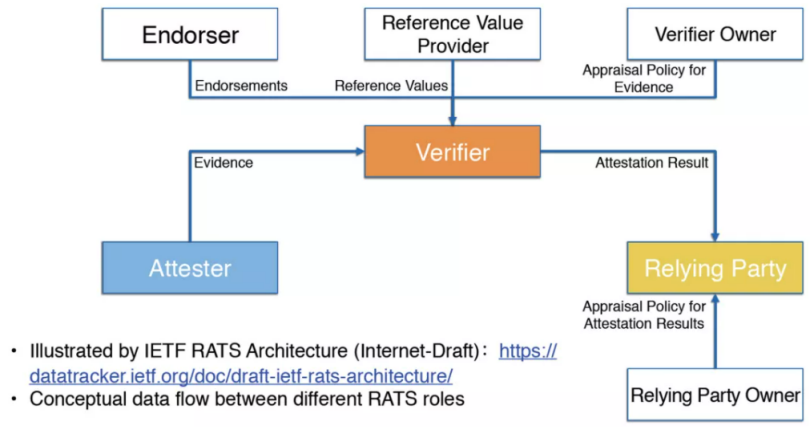

Figure 2.6: Remote Attestation (RATS) reference Architecture [13].

2.3 Attacker model

Modeling the role of attackers is an important topic in cyber defense since it helps to verify that security assessments are scientifically correct, especially for conceptual contributions that cannot be proven experimentally or when comprehensive testing is impracticable. Depending on how extensive the formalization is, the adversary might be an algorithm or a sequence of assertions about skills and aims. This umbrella encompasses a variety of techniques in several aspects of computer security. Adversary models are important in the realm of cryptography because they are used to prove the security of a certain cryptographic method or protocol [15].

Adversaries may be built with a variety of capabilities; each of these customizable adversaries is characterized as a new sort of attacker with unique skill sets, advantages, and downsides. Adversary models have also been used to codify a system or protocol assault. In the world of security, an adversary is an attacker, sometimes with hostile intent, who launches an assault against a system or protocol. Typically, the adversary's purpose is to disrupt or inhibit the correct operation of a secure system (for example, by compromising the system's confidentiality, data integrity, or availability).

Threats and associated protection goals for IT systems are typically organized as follows:

- Unauthorized gain of data, i.e., loss of **confidentiality**.
- Unauthorized modification of data, i.e., loss of **integrity**.
- Unauthorized impairment of functioning, i.e., loss of **availability**.

Protection from an omnipotent attacker is of course impossible. As a result, all of the procedures are simply approximations of perfect safety for participants from all potential attackers. The approximation is decided by the definition of an attacker's maximum considered strength, which is molded into a so-called attacker model.However, it is important to note the differences in Attacker Model, an Attack and a Threat model.

There could be an observation attack and/or a modification attack in a broad sense of type of attack from either an outsider or an insider. For a Cloud Service Provider, the data should be isolated from the cloud administrator, the hardware, Guest OS - providing us vendor exclusion. Here, the Guest Admin, like us developers, have to be trusted. The Hardware provider, like Intel, AMD, Apple, etc also have to be trusted here. When we talk of the Confidential Cloud Computing, it is assumed that the Hardware provider has no access to the data and cannot breach the confidentiality, or integrity of the data.

Attacker Model - e-health application on Cloud

Potential Attackers and their potential to attack the system:

- Malicious user - external (outsider) - Hacker, etc.
- Cloud Service Provider
  - executing malicious hypervisors (event injects, memory replay, and memory aliasing, among others).
  - launching harmful guests (fake identity, unauthorized memory access, etc.).
  - running malicious host programs (unauthorized memory access, etc.).
  - putting malicious software (unauthorized DMA to guests, etc.).
  - launching the guest wrongfully (insecure configuration enabled, deliberately modified initial guest image, etc.).
- Malicious user - internal (insider) - Admin, etc.

For the e-health project, it is easy to assume that we should not have to trust the CSP with anything, except for the infrastructure that can be attested remotely. However, the guest OS, depending on the model of deployment, has to be trusted. The Cloud Admin (us, developer) is also to be trusted and not everyone should be able to make changes to the database schema, infrastructure, etc. There should be no way the Disks attached to the VM are accessed by anyone unauthorized. The network capabilities of the VM/deployed model should make sure that it is not intercepted by an attacker, and even if it is done, the data should be protected from attacks on its integrity and confidentiality. As crucial as availability, getting the right data via the right channel precedes it. Any changes to the deployment must be approved by the Cloud Admin (us, developers) via a Key or IAM functionality. A major contribution of the cloud-secure computing model is to the protection of data while it is being processed. So, in theory, this should give us protection for various observing attacks as explained in the later sections.

2.4 Trusted Execution Environments (TEEs)

In this section, we delve deeper into the topic of Trusted Execution Environments and into the various products/services provided by some companies - Intel, AMD, Apple, etc. Apple released the iPhone 5s in 2014, which included a Secure Enclave Processor, which was isolated from the rest of the system. This chip held sensitive information such as Apple Pay, iCloud keychain passwords, Face ID, and Touch ID biometric data. Cryptographic signatures were also saved for app verification. To prevent problems from being exploited, the memory was physically segregated from the rest of the terminal's memory. Third-party programs couldn't access the store, and even if the application process was hijacked, access to the iCloud account-authenticated personal storage was impossible. This was the first large commercial enclave, also known as a Trusted Execution Environment (TEE). This was published in a recent article [16].

To run user-specified code and data inside a secure enclave that even an attacked OS or hypervisor cannot access, TEEs rely on special CPU features [6]. It's the perfect hardware-level basic for safely running applications on unreliable platforms like public clouds, network edges, and external service providers. The most well-known TEE is Intel's Software Guard Extensions (SGX), which was introduced in 2015's Skylake CPUs and is present in the majority of Intel server processors. AMD's Secure Encrypted Virtualization (SEV) technology, which turns each protected virtual machine into a secure enclave, is also present in

AMD EPYC CPUs (as of 2017). Typically, when memory pages are not in use (such as when swapped to the disk), a TEE automatically encrypts them. The encrypted memory pages are decrypted and stored in a secure memory location that only the owner process can access, such as the enclave page cache (EPC). To ensure optimal efficiency and powerful security, use AES encryption.

2.4.1 Intel SGX - Intel Software Guard Extensions

Intel SGX is a set of extensions to the Intel architecture that aims to guarantee the integrity and confidentiality of security-sensitive computations carried out on a computer machine where all privileged software (such as the kernel, hypervisor, etc.) is possibly malicious [17]. Intel SGX is the most widely used TEE implementation. Private Reserved Memory (PRM), a section of the current system memory, is set aside for SGX implementation. To separate PRM accesses from operating systems, virtual machines, or other privileged system routines, Intel expanded its x86 instruction set. The user constructs an isolated container known as an "enclave" and runs the secret code inside of it when it wishes to do a secure computation. PRM is used by an enclave to host data and code. An Intel service can test the cloud provider using a third-party remote attestation protocol to determine whether it is utilizing an approved SGX-enabled CPU before establishing an enclave. The user can securely upload their code to the enclave after creating it. After computing the plain text data and encrypting the outcome, the user can return the decrypted data to the untrusted cloud components. When other programs attempt to access the memory of an enclave while it is running, the CPU will reject the request and return 0xFF, also known as the abort page in SGX. The untrusted component and the enclave component are often present in an SGX application. Fig. 2.2 shows in detail the runtime execution of Intel SGX [6].

It enables users to isolate applications in secure memory enclaves. These applications are secured against malware and unauthorized user access as it is embedded into the CPU, which means that even if the operating system (OS) or hypervisor layers are hacked. Superior data protection is the end result, which is ideal for businesses that handle sensitive data, especially those in the healthcare and financial services industries. Thus, this seems perfect consideration for our e-health data processing scenario. Hackers are quick to enter the stack in search of newer flaws as software layer security is enhanced.

The very first layer, silicon, should be secured by businesses initially. Passwords, client information, patient records, financial information, and encryption keys can all be safely stored in the dependable enclaves offered by Intel SGX as demonstrated by researchers earlier [18, 19]. SGX uses native CPU security instructions to encrypt portions of memory.

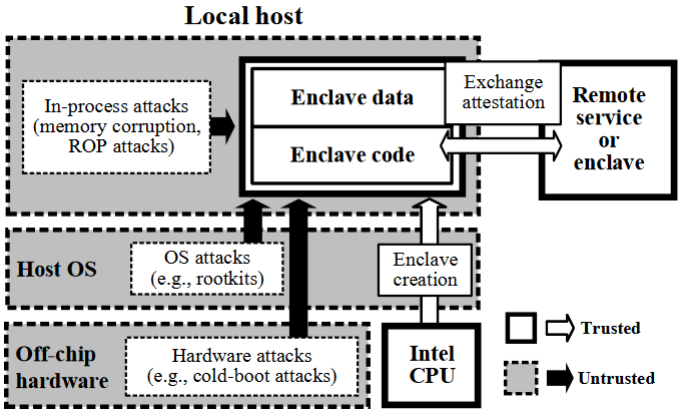

Figure 2.7: Simplified - Intel SGX Architecture [20].

Intel SGX is a type of hardware-based encryption that enables users to secure their most

sensitive data by encrypting it and storing it in a highly secure environment. It is, therefore, the one that is employed in various confidential computing services by Microsoft Azure, IBM Cloud Data Guard, Baidu, Alibaba Cloud, and Equinix [5].

SGX - Strengths	SGX - Shortcomings
Intel SGX provides memory integrity protection, which is perfect for our e-health data processing scenario [21].	Repeated Switching between the application and the enclave results in substantial performance costs while using SGX [22].
Intel SGX prevents the execution of user-supplied code by requiring Intel-signed code to load in release mode.	All of those options define a code region as readable and executable in order to get past this restriction and load user-supplied code into it.
Only the Intel CPUs and the code executing in the enclave(s) are to be trusted thanks to SGX's threat model.	Memory pages can only set their attributes once. This adds code injection attacks, which have been handled in traditional applications for more than ten years, and leaves all injected user code on pages with full permissions.
Programs are protected by SGX from three different sorts of assaults on the same host: attacks from untrusted application code running in the same process while outside the enclave; attacks from other programs running on the same host; and attacks from off-chip hardware [20].	All assessments demonstrate that SGX-based solutions are having a major performance impact.

Table 2.1: Intel SGX Pros and Cons.

2.4.2 Intel TDX - Trusted Domain Extensions

As explained by authors in [23], the fourth generation Intel Xeon Scalable Processors include TEE capabilities thanks to an architectural extension called Intel Trust Domain Extensions (TDX). To provide cryptographic isolation and security for Virtual Machines (VMs), also known as Trust Domains (TDs) in the TDX terminologies called the Secure-Arbitration Mode (SEAM). The threat model presumes that privileged software, such as host operating systems or hypervisors, may be untrustworthy or malicious. TDX enables TD owners to confirm the legitimacy of distant platforms while also aiming to secure the confidentiality and integrity of CPU state and memory for specified TDs. VT (Virtualization Technology), MKTME (Multi-key Total Memory Encryption), and the TDX Module are only a few of the methods used to create TDX. For remote attestation, TDX additionally uses Data Center Attestation Primitives (DCAP) and Software Guard Extensions (SGX).

Attacker Model - Intel TDX

Cross-domain attacks by an outsider malicious user are mitigated by TDX's enforcement of cryptographic isolation among the security domains. It ensures the privacy and integrity of TD's memory and virtual CPU states, and remote attestation gives tenants evidence that TDs are actually running on genuine Intel processors with TDX support which is good for

our e-health data processing scenario, as long as we trust Intel as a provider. Because this encryption is carried out at the cache line level, it is impossible for external devices to read from or modify the TD's private memory without being noticed. Hence, protecting the data from a user's observing or modifying attack. By controlling the virtual CPU states of TDs during context transitions across security domains, TDX guards against concurrently running programs. Additionally, it shields TD's execution from host intervention and has the ability to detect malicious alterations to the virtual CPU states. However, data located in shared memory areas are not protected in terms of confidentiality and integrity. To solve these problems, trusted I/O virtualization will be a part of TDX 2.0 in the future [23].

The Adversary attacker model of TDX:

- Through the host-side interface functions of the TDX Module, adversaries are able to construct, initialize, measure, and disassemble TDs which could result in a Denial-of-Service (DoS) attack.
- Adversaries have the ability to manage the physical memory pages, CPU time, and physical/virtual devices assigned to TDs.
- Adversaries can attempt to read from and write to any location in memory, interrupt TDs at any time, and change the settings of the Input/Output Memory Management Unit (IOMMU).
- Physical attacks that roll back arbitrary memory areas are undefended. The secret key material built inside the processor chip's fuses, however, shouldn't be accessible to attackers.
- Fault injections and side-channel attacks like power glitches, time, and power analysis are not included in the threat model's scope. Attacking TDX attestation is allowed since it threatens the trust paradigm and makes it possible for attackers to create a fake TEE for the purpose of obtaining sensitive information from tenants.

Memory is protected at various granularities via SGX and TDX. However, TDX and SGX are within the same TCB on the same platform. They can therefore locally attest to one another. The remote attestation tool offered by SGX is used by TDX. Within a Quoting Enclave, the attestation report of a TDX platform can be verified and signed. It's important to note that executing an SGX enclave inside of a TD is currently not permitted because doing so can result in UD exceptions when ENCLS or ENCLV instructions are invoked. The in-depth analysis of the TDX Attacker model reveals the various improvements needed and the loose ends present in the current version of the TDX. The proper TDX Architure can be observed in Figure 2.8.

Most of the new Intel Home-PC-based processors after the 12th Gen Intel Core i3/5/7 processors will now be equipped with Intel TDX as released by Intel in one of its reports from 2022 with the launch of its first-of-many Intel 12th Gen mass-market home processor. This shows that Intel SGX has been Deprecated [24].

2.4.3 AMD SEV - AMD Secure Encrypted Virtualization

There has been an exponential increase in how systems are now more consolidated than ever, making their architecture and design more complex. In addition to raising the attack surface and allowing multiple software applications to share hardware and resources like memory, consolidated systems are vulnerable when it comes to security. With a lot of privileged bug-free code and a broad attack surface, this combination creates a security paradigm that is a lot more vulnerable to security breaches. The AMD architecture's feature

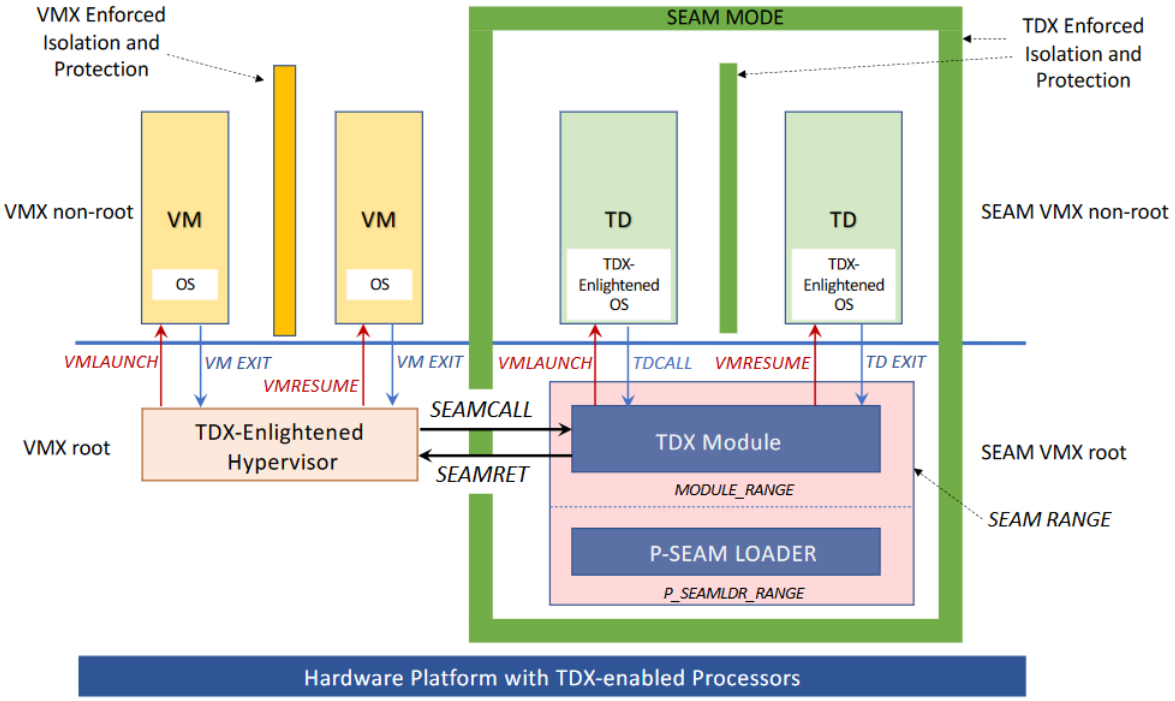

Figure 2.8: Intel TDX Architecture [23].

called Secure Encrypted Virtualization (SEV) is designed to better handle the complexity and isolation requirements of newer systems. Code and data can be encrypted with the use of SEV, which also provides a comparatively new security paradigm that allows code to be cryptographically isolated from more privileged programs, such as a hypervisor, and improves isolation through the use of cryptography. The SEV is an extension of the AMD-V architecture which supports running multiple VMs under the control of a single hypervisor. In a multi-tenant cloud environment, it shields sensitive data kept in VMs from privileged applications or administrators. For the purpose of ensuring cryptographic isolation between virtual machines and the hypervisor, SEV depends on AMD Secure Memory Encryption (SME) and AMD Virtualization (AMD-V).

The ability of guest VMs to select which data memory pages they want to be private is one of SEV's important characteristics. The option is done using the common CPU page tables, and the guest has complete control over it. Although shared memory may be encrypted using the hypervisor key, private memory is encrypted using the guest-specific key. With this feature, virtual machines (VMs) can assign certain memory pages as confidential, and others as being used for communication with other virtual machines or the hypervisor. The guest would typically map all of its code and data as confidential, except for certain shared pages that it chooses to expose. Some memory types, such as instruction pages and page tables, must always be private for SEV hardware to maintain security and safeguard the VM. The SEV model isolates code running at several layers, such as the hypervisor and the guest, such that neither can access the resources of the other. SEV isolates these levels using cryptographic isolation, even though the hypervisor level is normally more privileged than the guest level. This allows the lower privileged code more protection without requiring complete trust in the high privileged code, which the less privileged code depends on to start up and run. It is still possible to communicate between the hypervisor and the guest, but the channels are strictly controlled [25].

As a result, SEV technology is based on a threat model where an attacker is capable of

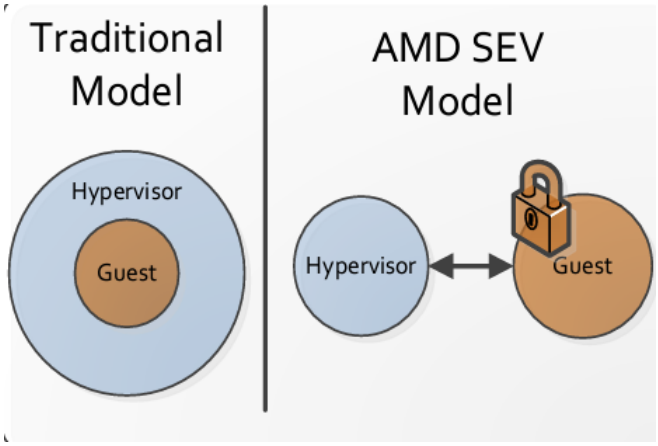

Figure 2.9: SEV Security model [25].

running malware not only at the user level of privilege on the target computer but also at the higher privilege level of the hypervisor. Also, the attacker may physically access the device, including the DRAM chips. SEV offers additional guarantees in each of these situations to aid in isolating the data and code of the guest virtual machine from the attacker. SEV offers enhanced security isolation that is rooted in the hardware itself, which may be used to enhance the level of security in various IaaS cloud deployments, like in our scenario of e-health data processing confidential cloud IaaS stack. SEV secures data-in-use, enabling client workloads to be protected cryptographically from each other as well as from the hosting software. Existing security solutions like Microsoft's BitLocker and LUKS can only protect data at rest in hard drives. Even a Hypervisor Guest administrator with malicious intents at a cloud data center would not be able to get access to the information in a hosted VM.

Another important piece of tech, SEVGuard [26], separates userspace apps using SEV to the ones using Intel's SGX. SEVGuard also sends the syscalls to the host OS as in the previous techniques. SEV provides the option to alter memory attributes at any moment. Because SEVGuard lacks a secure storage mechanism or a shielding layer, it is susceptible to Iago attacks.

Adversary Model

In SEV, an effective adversary is assumed to be able to completely compromise the system software, including the hypervisor and the host system kernel [27]. As a result, the adversary is able to read as well as modify the entire system memory while it is running, hence being able to access the confidential e-health data. Additionally, they have the capacity to create SEV VMs, commodity VMs, and malicious host processes. Additionally, the adversary has the ability to track all network activity, including SEV VM traffic, by injecting packets and acting as the host. The adversary's objective is to compromise SEV VMs or modify network traffic directed at SEV VMs in order to control them or even steal their sensitive data. Additionally, the attacker has physical access to the server, which gives them the ability to carry out non-intrusive physical attacks like bus snooping or even cold-boot attacks [28].

Summary

An individual, transient Advanced Encryption Standard (AES) key is given to each virtual machine (VM), and this key is used to encrypt runtime memory. Data written to or read from the main memory is encrypted or decrypted by the AES engine in the on-die memory controller. Additionally, SEV offers a remote attestation method that enables the owners of

virtual machines to confirm the validity of the SEV platforms and the launch measurements of their machines. The attestation report is created by the PSP and is sealed with an AMD-verified attestation key. The embedded platform/guest measurements and the attestation report's veracity can both be checked by the VM owners. SEV has been released by AMD in three generations. The confidentiality of a VM's memory is the only thing the first-generation SEV safeguards.The third version SEV-SNP (Secure Nested Paging) provides integrity protection to prevent memory corruption, replay, and remapping attacks.Reverse Mapping Table (RMP)-based memory integrity protection is specifically provided by SEV-SNP. To prevent unauthorized access, RMP keeps track of who owns each page and who has access to it. By separating the guest address space into four levels and introducing the Virtual Machine Privilege Levels (VMPLs) feature, SEV-SNP also adds further security isolation within a VM.

2.4.4 AMD SEV-SNP - Secure Nested Paging (SNP)

The most recent AMD SEV solution for Confidential Computing is Secure Nested Paging (SEV-SNP). It advances AMD SEV and AMD SEV-ES (Encrypted State) aspects to offer protected VMs improved security, more varied usage models, and other features. First- and second-generation AMD EPYCTM processors support SEV and SEV-ES (2017). Since 2021, third-generation AMD EPYCTM processors also feature SEV-SNP [29]. It is made to protect a virtual machine from a corrupt hypervisor when needed. Hence, it is beneficial in scenarios where the hosting environment cannot be trusted, such as public clouds.

As shown by the Fig. 2.10, the measurements of TCB in SEV-SNP are:

- AMD firmware and microcode - Security processor boot loader, Security processor OS, SEV-SNP firmware, and Microcode for x86.
- SEV-SNP Guest - Launch metadata and its measurements, Guest configurations, and configuration of x86 runtime.

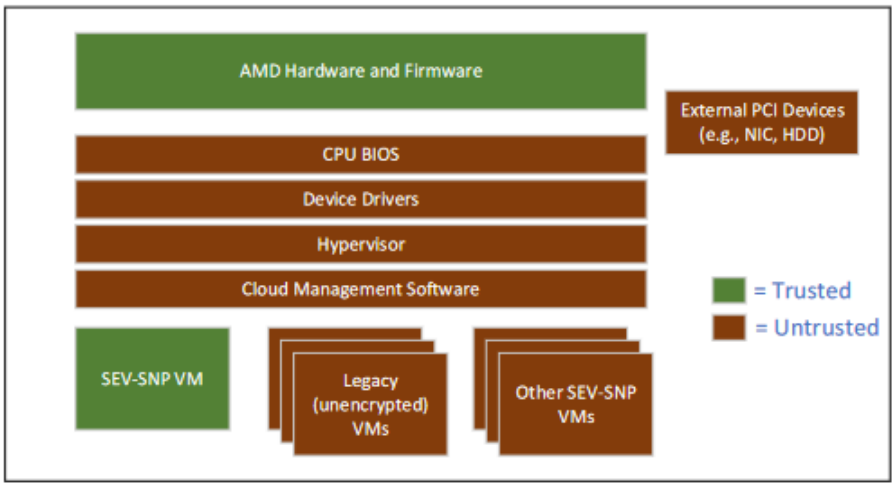

Figure 2.10: Measurements of Trusted Computing Base (TCB) [29].

2.4.5 TCX - Trusted Container Extensions

In [27] the author Brasser and their team introduce a new concept for container security architecture. It also enables confidential computing for container workloads by fusing the manageability and agility of standard containers with the robust protection guarantees of

hardware-enforced Trusted Execution Environments (TEEs). TCX protects container workloads and the data they process while outperforming existing methods in terms of performance. Built on top of AMD Secure Encrypted Virtualization (SEV), it guarantees the integrity and confidentiality of data and services throughout deployment and enables secure communication between protected containers as well as with outside parties. In accordance with other TEEs, the authors here, presume that this limited collection of hardware and software components is reliable and trustworthy by default.

2.4.6 Arm TrustZone

Arm TrustZone[30] is a system-wide method of embedded security for ARM Cortex-based processor systems. It enables a safe world and a less secure world to run simultaneously on a single core. Hacking can take many forms, from Distributed Denial of Service (DDoS) attacks to illegal access to internal networks, when a device is connected to the internet. Arm developed the Arm TrustZone technology to address the security concerns for embedded systems. The foundation of TrustZone is the least privilege principle, which states that system components should not have access to a resource unless absolutely essential. The software known as "core logic" (for Cortex-M processors) or the "secure monitor" (for Cortex-A processors) is used to perform tasks that must be performed across safe and non-secure environments. Assets can be shielded from both hardware and software attacks by building a security subsystem. A trusted execution environment (TEE) is a secure system environment that can designate certain memory locations for security needs, such as Point-of-Sale (POS) systems and Digital Rights Management (DRM). Regardless of privilege level, the non-secure OS cannot access the secure parts of the TrustZone. The Secure Boot Sequence, which is part of TrustZone, validates the secure boot images.

The two operating systems can communicate once the machine has done booting up via a monitor kernel mode, which functions similarly to a context switch. No device can be totally resistant to hacking, but TrustZone makes it considerably more difficult. Running a full OS in a safe environment has the advantage of making development more complex, but all procedures must be properly designed to preserve security continuity. Validation is necessary for operational modes and mode changes, and programmers must still write code judiciously and implement reasonable security precautions [30].

For trustworthy kernel components, ARM's TrustZone creates a secure environment. In contrast to SGX, TrustZone creates a trusted channel from the trusted kernel to additional on-chip peripherals. It also divides the hardware into trusted and untrusted worlds [20].

2.4.7 Arm Confidential Compute Architecture (CCA)

The Armv9 architecture featured the Confidential Compute Architecture (CCA) [31] and is well summarized by authors in [23]. Traditionally, Arm TrustZone has two distinct worlds - the Normal World and the Secure World - that enable secure execution. Software in the Normal World cannot access data in the Secure World because of TrustZone. The Realm World and the Root World are two new worlds that the CCA adds to the Realm Management Extension (RME). The TrustZone and other security domains, such as host operating systems, hypervisors, other Realms, and the Realm World, are isolated from workloads by the Realm World, which offers mutually distrusting execution environments for private VMs. Granule Protection Tables (GPT), an addition to the page table that keeps track of each page's ownership across various worlds, are used by CCA to ensure address space separation. Hypervisors or operating systems cannot directly alter the GPT because it is created and managed by the Monitor in the Root World. By changing the GPT, the Monitor is able

to dynamically shift physical memory across various worlds. In order to assess and confirm the CCA platform and the initial condition of the Realms, CCA also offers attestation.

2.5 TEEs Comparison - Intel SGX and AMD SEV

The popular TEEs employed by the CSPs are only Intel SGX and AMD SEV. They are also the ones which are most mature of all the other TEEs we have seen. The Intel TDX is very close but since it is not employed by any CSP at the time of writing this report, we stick with SGX and SEV. As detailed in [21], the various technical differences between Intel's SGX and AMD's SEV are summarized in a tabular form.

Intel SGX	AMD SEV
The initial architecture emphasized microservices and light workloads. (A small amount of encrypted memory that was mostly found in mobile and desktop CPUs)	The first design emphasized the cloud and IaaS. (Server family CPUs have a large quantity of secure memory)
Major software modifications and code reworking are required. (Not appropriate for securing older apps)	It does not need any program modifications or code restructuring. (This is appropriate for safeguarding older apps)
SGX operates on ring 3 and is not ideal for workloads with a high number of system calls.	SEV works with ring 0 and is ideal for a larger range of workloads, particularly those with a high number of system calls.
SGX is appropriate for tiny yet secure workloads. (The SGX has a tiny TCB)	SEV may be used to secure old, big, and enterprise-level applications. (SEV has a high TCB)

Table 2.2: Differences in Intel SGX and AMD SEV (Security and Vulnerabilities) [21].

Intel SGX	AMD SEV
Memory Integrity is protected.	Does not protect memory integrity.
Memory Side Channels are a threat.	Memory Side Channels are a threat.
Denial of Service Attacks are possible. (The operating system handles system calls.)	Denial of Service Attacks are possible. (VM Requests are handled by the Hypervisor).
TCB of a small size. (TCB stands for CPU package.)	Large TCB (the VM's OS is housed within the TCB).
Synchronization attacks are possible. (TOCTTOU, Free-After-Use)	A bug in the AMD Secure Processor Firmware has been discovered. (FALLOUT and MASTERKEY)

Table 2.3: Differences in Intel SGX and AMD SEV (Function and Use Cases) [21].

From what we learned about Intel SGX and AMD SEV, it is understood that Intel SGX is a better choice of the two options. It is so because Intel SGX carefully isolates trusted and untrusted environments, offers a restricted and secure enclave gateway, imposes memory access control, and employs memory integrity protection, making it an appropriate TEE for securing workloads that deal with security-sensitive data [21]. Hence, it concludes that we should prefer a CSP provider who provides us with Intel SGX technology as the TEE provider.

3 Cloud Service Providers

3.1 AWS- Amazon Web Services

AWS has various services that can help us design solutions for database storage, compute power, content delivery, etc. It does so with high levels of sophistication, flexibility, reliability, and automation. As for our requirements for the e-health data processing platform from a CSP, all these are essential.

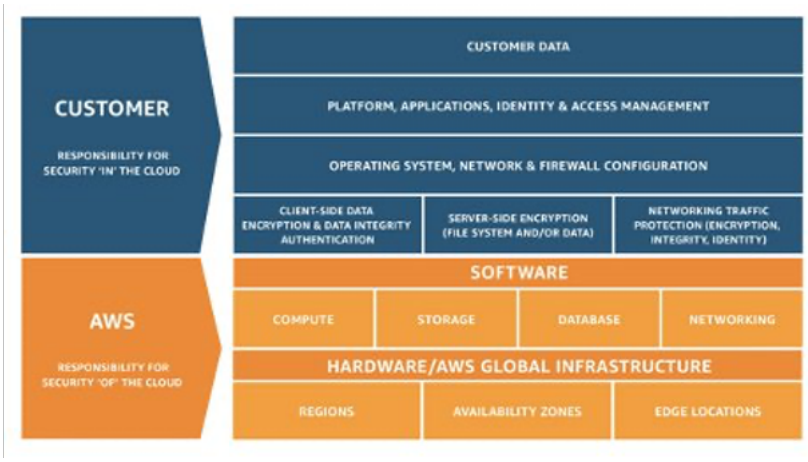

Figure 3.1: Shared Responsibility Model - AWS [32].

3.1.1 AWS Nitro System

In the AWS domain, confidential computing refers to the usage of specialized hardware and related software to shield client code and data from outside access while processing. There are two independent security and privacy elements in confidential computing [33]:

- GOAL 1: Customer safety from cloud service providers and cloud system software.
- GOAL 2: Dividing client tasks into parts with higher and lower levels of trust.

The AWS Nitro System [33] is the proposed solution by the developers. One good example of how they have created and innovated on behalf of their customers to give more confidentiality and anonymity along with privacy for their applications is The Nitro System,

the foundational technology for all newer Amazon EC2 instances. The **Nitro Cards**, **Nitro Security Chip**, and **Nitro Hypervisor** are the three primary components of the Nitro System. A Nitro card for Amazon Virtual Private Cloud (Amazon VPC) and another for Amazon EC2 instance storage, like others are specialized hardware elements with computational capabilities that perform I/O operations. Key virtualization functions can now be moved off of EC2 servers thanks to Nitro Cards. In order to measure and validate the Nitro System cryptographically, AWS developers have built a hardware-based root of trust into the system using the Nitro Security Chip. This offers a level of trust that is considerably higher than what can be achieved with conventional hardware or virtualization systems. A minimal hypervisor called the Nitro Hypervisor controls memory and CPU usage and provides performance that is equal to that of bare metal as experimented in [34].

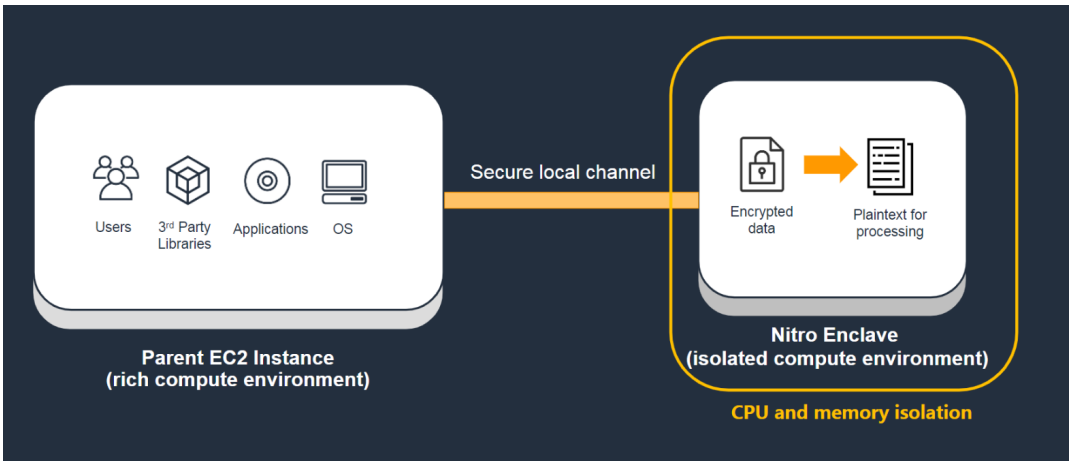

Figure 3.2: Overview - AWS Nitro Enclave [35].

3.1.2 Nitro approach to Confidential Computing

The Nitro System offers three kinds of protection in general. The first two focus on - GOAL 1 (Customer safety from cloud service providers and cloud system software). The third one focuses on GOAL 2 (Dividing client tasks into parts with higher and lower levels of trust).

1. **Protection from cloud operators** - With no operator access to the Nitro System, AWS has structured its processes to guarantee workload confidentiality between clients and AWS. Only a small number of authenticated, authorized, and audited administrative APIs are available for use by any AWS operator who needs to perform maintenance on an EC2 server.

2. **Protection from AWS system software** - For bare metal instances, the Nitro System's innovative design uses low-level, hardware-based memory separation to prevent direct access to customer memory and to do away with the requirement for a hypervisor.
    - For **virtualized** EC2 instances - The Nitro Hypervisor collaborates with the underlying hardware-virtualization systems to build virtual machines that are separated from the hypervisor as well as from other virtualized EC2 instances, as seen in the Fig. 3.3.
    - For **bare metal** EC2 instances - Customers see direct and privileged access to the entire underlying main system board for bare metal EC2 instances, as depicted in Figure 3.4. The EC2 server lacks a hypervisor for bare metal instances, allowing customers to access physical resources for low-level hardware features

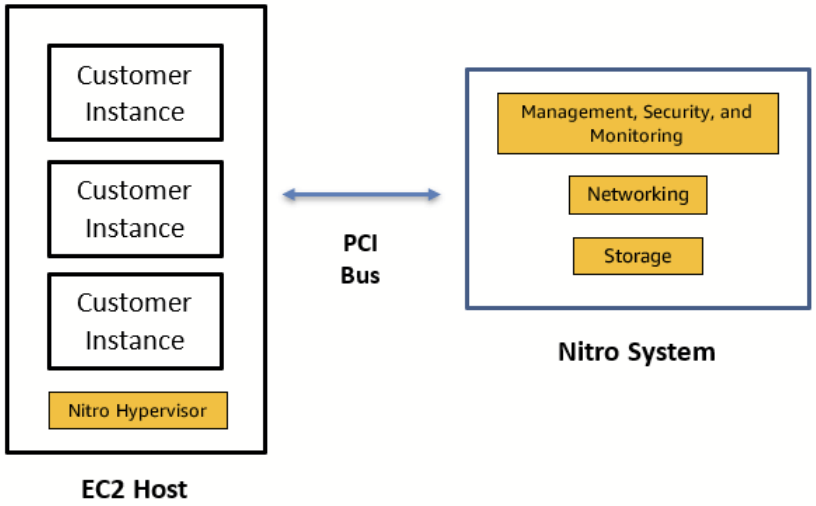

Figure 3.3: Virtualized EC2 instances - AWS [33].

like performance counters and Intel VT, as well as licensed applications for non-virtualized environments or hardware-only running, as seen in the Fig. 3.4.

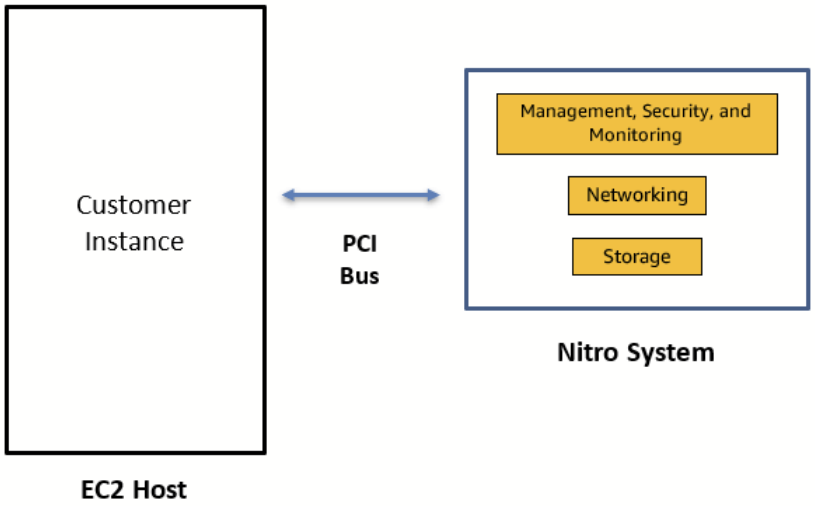

Figure 3.4: Baremetal EC2 instances - AWS [33].

3. **Protection against customers' own operators and software for sensitive computing as well as data aspects** - The second aspect of confidential computing is offered by Nitro Enclaves. Nitro Enclaves is a hardened, fully isolated computing environment that a customer's EC2 instance connects to. It prevents interactive access to any user or application. Nitro Enclaves' cryptographic attestation capabilities ensure software deployment is certified. This allows customers to separate their systems with varying levels of trust while maintaining security from the cloud operator. It also protects sensitive code and data from AWS operators and other software.

Attestation with AWS

The attestation procedure employs a set of metrics that are exclusive to each enclave. These measures can be used to set access controls in external services that allow the enclave to perform particular cryptographic operations [36]. An enclave can use the Nitro Enclaves SDK to obtain a signed attestation document via the Nitro Hypervisor containing its unique measurements. This document can be added to enclave requests to an external service. To assess whether to provide the enclave access to the requested action, the external service can check the measurements supplied in the attestation document against the values in the access policy. Nitro Enclaves has built-in support for AWS KMS (Key Management Service) attestation. AWS KMS is capable of ingesting attestation documents supplied by an enclave. You may conduct AWS KMS activities such as Decrypt, GenerateDataKey, and GenerateRandom directly within the enclave using the AWS KMS APIs available in the Nitro Enclaves SDK.

As evident from the presentation [37], the whole attestation is happening on AWS itself. For this, one is supposed to trust AWS with the attestation as well. This is a huge amount of trust and we should try and find an alternative where we can get the attestation report (and not PCR values, as in AWS) directly from the actual hardware enclave, without the meddling or verification of the CSP.

From our research and related work study, AWS Nitro Enclaves proved to be really efficient and provide excellent scalability capabilities. Although software implementations of these sorts of components exist, hardware is typically thought to be more secure and difficult to tamper with. Having said that, more and more hardware vulnerabilities are emerging and becoming a worry for enterprises that manage highly sensitive data, like our use-case, e-health data.

3.2 GCP - Google Cloud Platform

GCP is a collection of cloud computing services that came out of the initial Google App Engine framework for hosting web applications from Google's data centers. GCP has evolved into one of the main cloud computing platforms on the market since the debut of Google App Engine in 2008. GCP is regarded as the third biggest cloud provider in terms of revenue behind AWS in the first place and Microsoft Azure in the second [38]. Conventional security models cannot secure today's cloud-based, distributed environments and workforce. To protect the on-site workforce and workloads, Google Cloud enables us to build a zero-trust model, in which trust in users and resources is established through numerous means and continuously confirmed [39]. These solutions include but are not limited to, BeyondCorp Enterprise, Work Safer, Certificate Authority Service, VPC Service Controls, and Titan Security Keys.

There is support in GCP for -

- Confidential VMs and Compute Engine
- Confidential Google Kubernetes Engine (GKE) nodes
- Validation of Confidential VMs using Cloud Monitoring
- Dataproc Confidential Compute
- Ubiquitous data encryption with STET

3.2.1 Confidential VMs - Google Cloud Platform

As established in the previous chapters, Confidential Computing facilitates the protection of data in use with the help of hardware-based TEEs. TEEs are isolated, secure environments that make sure there's no unauthorized access or unwanted changes to data and applications while they are in use. End-to-end encryption states are as follows:

- Encryption-at-rest - data is protected while it is being stored.
- Encryption-in-transit - data is protected while it is traveling between two places.
- Encryption-in-use - data is protected while it is being processed, achieved using CC.

In the domain of GCP tools, CVM is a Compute Engine VM that makes sure your data and apps remain secure and confidential even when in use. It helps avoid exposing sensitive data or workloads while processing. It is run on AMD EYPC processors that support AMD SEV. It provides -

- Isolation - During VM setup, the AMD Secure Processor (AMD SP) generates encryption keys, which are then stored exclusively on the AMD System-On-Chip (AMD SOC) and Google (GCP) cannot access it.
- Attestation - It uses Virtual Trusted Platform Module (vTPM) attestation wherein a launch attestation report event is produced each time an AMD SEV-based Confidential VM boots up. This is software-based.
- High Performance - It is offered by AMD SEV for more intensive processing operations with there being minimal effect on most workloads, say around 0-6 percent decrease in performance [40].

In the GCP domain, the term used to indicate an enclave is a Confidential Space. It is made to enable participants to exchange confidential data under a workload that has been mutually agreed upon while maintaining the confidentiality and management of that data. Personally identifiable information (PII), protected health information (PHI), intellectual property, cryptographic secrets, and other types of data may be included in such data. Data is isolated by Confidential Space so that only the workload and the data's original owners can access it. A TEE used by Confidential Space has the purpose of only releasing data to authorized workloads. The workload and the data it processes are protected from an untrusted operator by an attestation method and a hardened OS image. It has three main components -

- A workload - a containerized image that executes on top of the confidential space image, which runs on CC.
- An attestation service - runs in the same region, and verifies the attestations of TEE by token provider (OpenID Connect). These tokens have the identification properties for the particular workload.
- A protected resource - such as a Cloud Key Management Service (Cloud KMS) that grants access to only authorized federated identity tokens by IAM, providing the conditions are met.

In such a system, there are three role types -

- The workload author - creates a containerized image with an application that can access restricted resources. The data and results are not accessible to the author and thus can't be controlled.

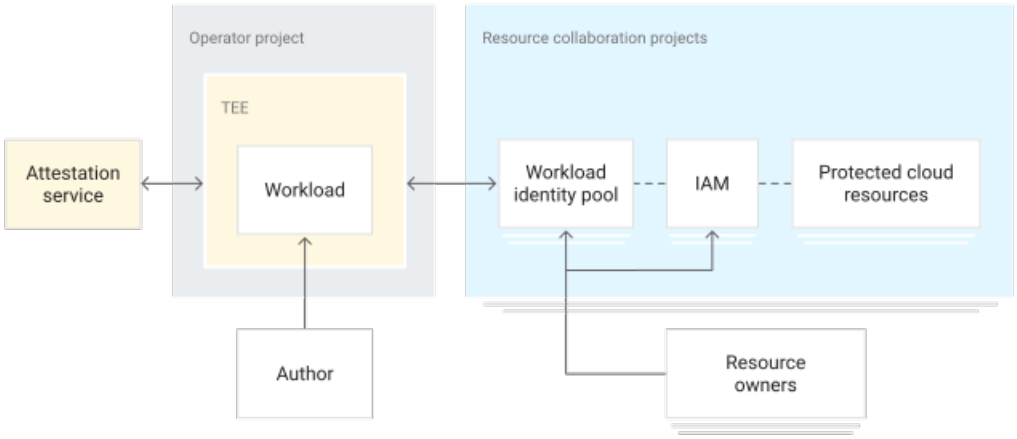

Figure 3.5: Confidential Space - GCP [40].

- The workload operator - the admin, who runs the workload in GCP and manages the resources like Compute Engine, etc. However, they can't access/modify the date or the results from its processing.
- The resource owners/data collaborators - the owner of the protected resource, can access their own data, its results, and who else can access it. However, they cannot access any other resource owner's data or their results.

3.2.2 Confidential Google Kubernetes Engine (GKE) nodes

Google Kubernetes Engine (GKE) is a managed Kubernetes service that allows you to leverage Google's infrastructure to install and run containerized apps at scale. This website is for platform administrators seeking a scalable, automated, and managed Kubernetes solution. Confidential GKE Nodes are created on top of the Compute Engine CVM, which encrypts the memory contents of running VMs. After confidential GKE Nodes is enabled on a cluster or on a node pool, the data in these workloads which are running on confidential nodes, is encrypted in use. Confidential GKE Nodes are based on the Compute Engine Confidential VM, which encrypts the memory contents of running virtual machines. One of the three states of end-to-end encryption is encryption-in-use.

WWhen Confidential GKE Nodes are enabled on a cluster or a node pool, data in workloads operating on the confidential nodes is encrypted in use. One can use the Access Transparency service to get visibility over the supposed control plane.

Attestation with GCP and GKE

Distributed participants may engage in an auditable signing process using Multi-Party Computation (MPC). The verified attestation provided by Confidential Space may assist in guaranteeing that all collaborators safely approve while never disclosing their secret signing keys to outside parties, including the platform operator.

Google Kubernetes Engine (GKE) encrypts client stuff at rest, including Secrets, by default. GKE maintains and manages this default encryption for you without your intervention. Application-layer secrets encryption adds an extra layer of protection to sensitive data saved in etcd, such as Secrets. Using this capability, you may encrypt data at the application layer using a key maintained by Cloud KMS. This encryption prevents attackers from accessing an offline copy of etcd. To employ application-layer secrets encryption, you must first establish

a Cloud KMS key and provide access to the key to the GKE service account. You can use a key that has any of the Cloud KMS protection levels.

The Attestation is software-based and is completely taken care of by Google. It is both a good and a bad thing to be abstracted from all the fine details. In our scenario, as we have the e-health data, security is a huge concern and we developers would like to know more about the Attestation process. There is also a huge amount of trust put into Google with the whole Attestation process. We don't get the report directly from the hardware enclave but just some values that are assuring but not enough for our serious e-health scenario.

3.3 OVHcloud

OVHcloud is a major participant in the world and the top European cloud provider, with 400,000 servers across 33 of its own data centers on four different continents. The Group has been utilizing an integrated model for the past 20 years, which gives us complete control over every step of our value chain, from designing the servers to running the data centers to orchestrating the fiber-optic network. Using this distinct strategy, OVHcloud is able to independently cover the whole range of use cases for its 1.6 million clients in 140 countries. In order to support its unrestricted expansion, OVHcloud now provides customers with cutting-edge solutions that combine excellent performance, predictable pricing, and complete data sovereignty.

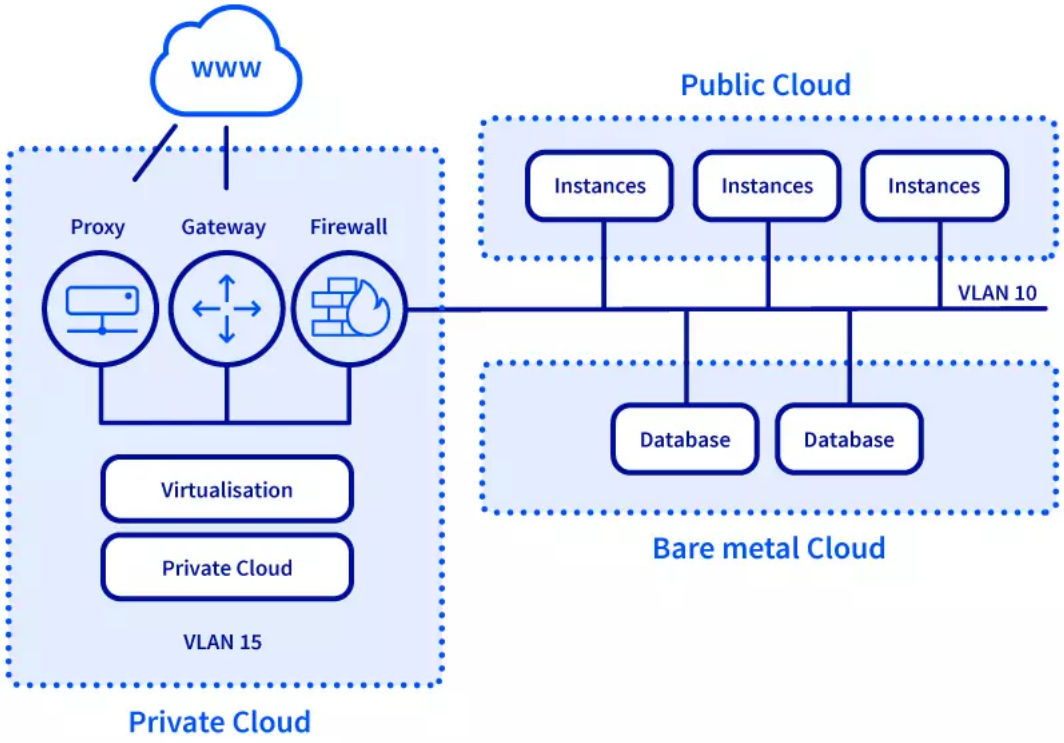

Figure 3.6: Multiple Service Integration in OVHcloud [41].

3.3.1 OVHcloud Bare Metal Servers - Confidential Computing

The new Advance-6 Bare Metal Servers from OVHcloud are powered by 3rd Generation Intel Xeon Scalable Processors (previously codenamed "Ice Lake") and Intel Software Guard

Extensions (Intel SGX). These innovative solutions boost speed while using Confidential Computing for data privacy, regulatory compliance, and enhanced data security. When performing machine learning procedures that use sensitive data, especially in the financial and medical industries, data processing security is crucial. Data streams must be protected, especially during workloads and communications with other parties. The BMS offering from OVHcloud might just be our answer to the security concerns raised by the other CSPs. As in a Bare metal server, there can be zero to no managed services.

- Intel SGX Technology - Intel Xeon E CPUs are used in advanced servers, which also have hardware and RAM encryption features. The program and the most sensitive data are shielded against change and disclosure in this way. With the help of these technologies, one can defend the data against tampering, overflow, and server-side spying.
- AMD Infinity Guard - AMD EPYC processors, which are based on Zen architecture, incorporate the sophisticated security capabilities necessary for the best defense against both internal and external threats. The data is safely stored in this way, and the performance of the system is seldom affected.
- Combine workloads and secure the data- One can isolate the programs from one another on servers with numerous CPU cores using secure enclave management to consolidate them. One can increase performance and security in this manner without compromising one's budget.
- Robust software solutions - The installation of a secure enclave is quick and easy using Fortanix, Red Hat Enarx, Open Enclave SDK, or VMware vSphere. For any infrastructure, it also provides the best performance, allowing one to combine security and speed.

As shown in Figure 3.7, one can set the enclave size quickly by enabling advanced processor protection features in the BIOS or OVHcloud Control Panel. After that, one can isolate a portion of the physical memory on one's server to create a secure runtime environment. A security enclave is this secluded area. By doing this, one will secure access to data that is being processed or running code. AMD Secure Encrypted Virtualization and AMD Secure Memory Encryption are security capabilities included in the AMD Infinity Guard architecture to safeguard virtual environments and memory integrity. Additionally, it defends against return-oriented programming threats (AMD Shadow Stack) and malicious agents (AMD Secure Boot).

In the case of this thesis project's e-health data processing scenario, we can take the help of its offering that uses Federated Learning. As shown in Figure 3.8, application processing can be combinedly secured. Utilize the computing power of our servers and select the appropriate machine for the job. One may process data from many sources while still ensuring that users maintain the confidentiality of their data by enabling strong security features. Federated learning is a secret automated learning technique (PPML). Without transferring data, it enables algorithms to learn from data sets spread across different devices or decentralized sites. As a result, organizations can create more accurate models, and sensitive data is not exposed to security risks.

Available options and services from OVHcloud[42]:

- Intel SGX (Intel Xeon E processor).
- AMD Infinity Guard (3rd generation AMD EPYC processor).

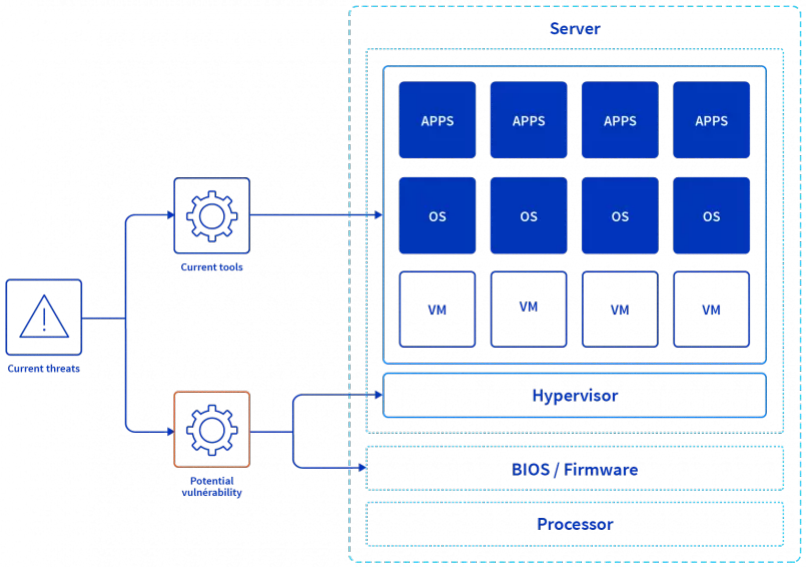

Figure 3.7: Hardware Security solution by OVHcloud [42].

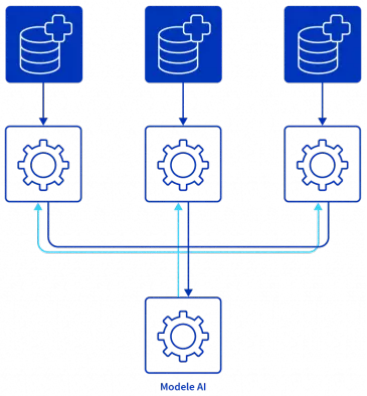

Figure 3.8: Federated learning model at OVHcloud [42].

- RAM and storage options.
- Claims of public and private bandwidth.

3.3.2 OVHcloud with SECURITEE - Case Study

As per the title of the case study [43], the most adaptability and scalability possible serve as a solid foundation for confidential computing. As it's already established as a problem, data is only effectively protected when it is at rest, in storage, or in transit - but not when it is being used or processed. This cybersecurity conundrum continues to provide a significant concern for consumers and providers alike. As claimed in [43], this perspective is altered by the solution offered by a startup SECURITEE, from Berlin, Germany. Using patented technology, the company develops the TEE based on Intel SGX that reliably safeguards all sensitive data against attacks, even when the data is being used. By isolating calculations in a hardware-based TEE, SECURITEE addresses a major issue that users of "Confidential Computing" - both on-premises and in the cloud - have long encountered. Users can access SECURITEE's solution through a Platform-as-a-Service (PaaS) paradigm.

It is now able to safeguard sensitive data during execution as effectively as it was previously possible in idle and transit states thanks to SECURITEE's patented new technology.

Developers and users benefit greatly from encryption during use since it enhances security and enables crucial data protection activities. The TEEs are impermeable, safeguarding any confidential data from a cloud assault just as securely as they would safeguard any on-premise resources. A solid infrastructure, or foundation, was required for the solution in order for the SECURITEE service to be delivered rapidly, effectively, on demand, and possibly via Kubernetes.

The alternative had to ensure complete security, complete GDPR compliance, easy scalability, and the possibility of building a special architecture inside of the cloud provider's existing infrastructure. This was and still is about much more than specific technical specifications: it's about being able to provide customers and users with a solution that is reliable in every way, abides by the GAIA-X initiative's tenets, and permits data sovereignty at every level of infrastructure.

DDoS attacks on OVHcloud report from 2021

The research by OVHcloud itself shows an overview of the attacks launched against the OVHcloud system in 2021. The scientific community can use this overview as an illustration of the issue that DDoS attacks continue to pose to a major European cloud provider. The specificity of the targets as well as the host is both globally related to the activity of DDoS attacks. The spread of attack vectors also appears to be tied to the target of these attacks' industry of business. TCP attacks will target services that are mostly dependent on HTTP, whereas UDP assaults are more likely to target video game services. The numbers given in the paper cannot be applied to all cloud providers because, for instance, different cloud providers may utilize different DDoS detection techniques or even have different business models.

The solution - published on March 2022

The open, reversible, scalable, and robust cloud architecture of OVHcloud hosts the SECURITEE PaaS product model. The solution is hosted in OVHcloud's completely owned German data center in Limburg a der Lahn, next to the German internet hub DE-CIX, which is part of a secured network to further increase high resilience and service continuity.

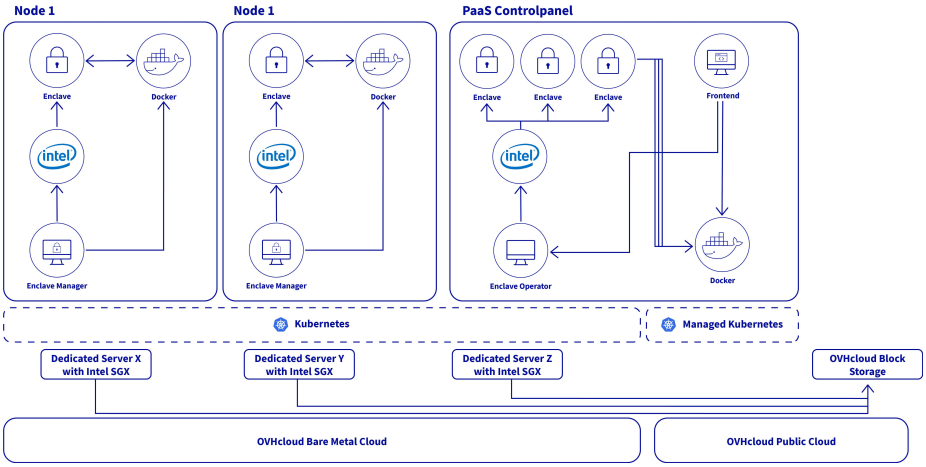

Figure 3.9: SECURITEE PaaS Solution [43].

For bare-metal servers, SECURITEE also utilizes the OVHcloud Managed Kubernetes service. Kubernetes serves as the foundation for the SECURITEE solution as an open-source platform for automating, deploying, scaling, and maintaining containerized applications. The

start-up can scale flexibly, easily update its service, and focus on its main business with the aid of the load balancers from OVHcloud and additional integrated hard disks.

The OVHcloud Public Cloud Block Storage is an additional component that enables the SECURITEE product's maximal functionality and widespread availability. This enables SECURITEE to raise the storage capacity during operation as needed and as demand dictates. The built-in replication capability provides additional security. The public cloud of OVHcloud's scalable, easily accessible services and direct access to the SGX hardware in the bare metal cloud allow SECURITEE to scale its own infrastructure as accurately and transparently as required from a security and user standpoint. Both companies have a similar goal for a safe digital ecosystem and a sovereign data infrastructure in Europe. Customers of SECURITEE can process their data in end-to-end safe settings while hosting it on OVHcloud servers. The basis of SECURITEE's distinctive product is effective data encryption even while processing, and OVHcloud offers the infrastructure for immediately distributing the solution to potential customers. In order to enable users to construct and administer secure environments—and even set up new enclaves as needed—OVHcloud offers the overall framework known as the SECURITEE Enclave Manager.

Attestation with OVHcloud

Confidential Computing with Intel SGX may be an important aspect of a compliance program, helping to decrease regulatory risk. Even a cloud provider like OVHcloud cannot access the data contained within an enclave. OVHcloud also provides attestation services, which provide clients with cryptographic confirmation that their workloads are executing on authentic Intel SGX hardware, the microcode is up to current, and the software load is precisely what is intended. Attestation ensures that our client's data is secure and compliant.

As we will see in Chapter 4, Europe is at the forefront of privacy and data protection with its GDPR and BDSG-new regulations. As a result, companies that handle personal or regulated data must use industry best practices and privacy-preserving technologies. Confidential Computing with Intel SGX can assist in lowering regulatory risk and ensuring data protection. Cloud providers like OVHcloud may access protected data contained within an enclave, and OVHcloud provides attestation services to validate workloads on real Intel SGX hardware, microcode, and software load, assuring data safety and compliance.

From our analysis and research, OVHcloud can be a strong choice, as it is strongly GDPR compliant and has servers in Germany, which means that the data stays in Germany. We may find out more about it when we implement their offering for our e-health use case with sample data.

3.4 Alibaba cloud

Alibaba Cloud, established in 2009, is one of the leaders in cloud computing and artificial intelligence, offering services to tens of thousands of businesses, programmers, and government agencies in more than 200 nations and regions. As part of its online solutions, Alibaba Cloud offers dependable and secure cloud computing and data processing capabilities since it is dedicated to the success of its customers.

3.4.1 Confidential Computing support

Confidential computing systems based on Intel SGX include the Inclavare Containers and the Alibaba Cloud ACK-TEE [44].

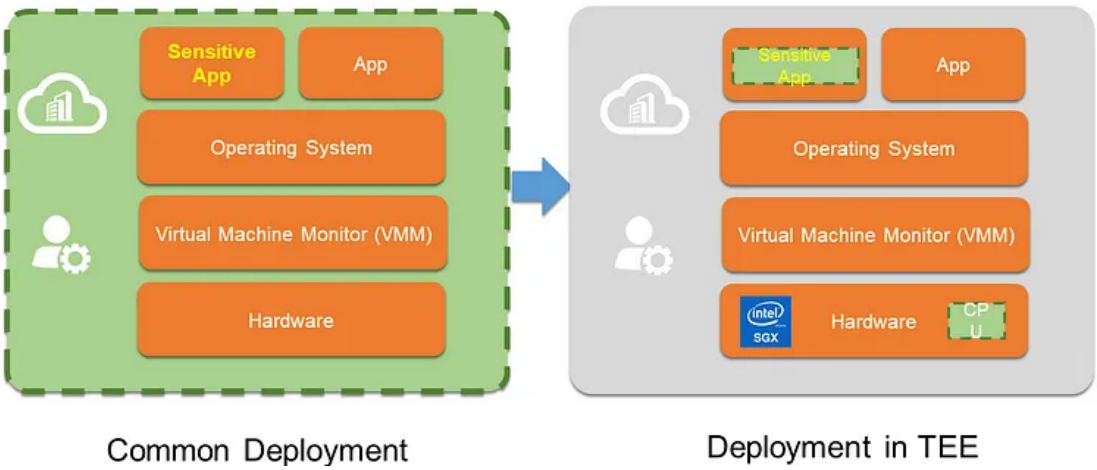

Figure 3.10: Intel SGX with a smaller TCB [44].

As shown in Figure 3.10, when deploying critical apps in the TEE of Intel SGX, TCB only has the TEE itself and the CPU. The TEE-based security mechanism increases the security of applications while lowering the attack surface.

Intel SGX divides applications into trusted and untrusted zones, with ECALL and OCALL functions to communicate between them. ECALL allows access to data in the untrusted zone, while OCALL allows access to data in the trusted zone. The process of any application development follows as - (1) Apply for secret key, (2) Install the environment - Intel SGX driver, SGX SDK, etc., (3) Use Trusted zone to indicate the code and data to be protected, compile the required files, divide the code into trusted and untrusted zones, (4) Build and compile code, (5) Run a container with Docker [9, 44].

Inclavare containers - open source

The word enclave's Latin derivation is inclavare. An open-source container runtime solution for confidential computing scenarios is called Inclavare Containers. It gives consumers the same ease of use as regular containers while lowering the high threshold of confidential computing. Additionally, it offers additional options and flexibility in terms of pricing and security. The medium article [44] provides a much more detailed explanation of the architecture of Inclavare Containers, the Shim-Rune (core and carrier) workflow, the client and the server signatures, multi-team cooperation, etc [9, 44].

3.4.2 Container Service for Kubernetes (ACK) based TEE - ACK-TEE

The latest version, ACK-TEE 2.0, is a container platform for secure cloud computing that intends to liberate the world from cumbersome confidential computing. It lowers the expenses associated with trusted and confidential application development, delivery, and management. It is based on hardware encryption technology. Collaboration Teams: Ant Financial Security Team, Cloud Security Team, Operating System Kernel Team, and Runtime Language Team Positioning support for native applications running in the TEE. In this version, an ordinary image is changed into a TEE image before being used in TEE. It offers trusted and secure service components through a controller like KMS-Enclave-Plugin [9, 44].

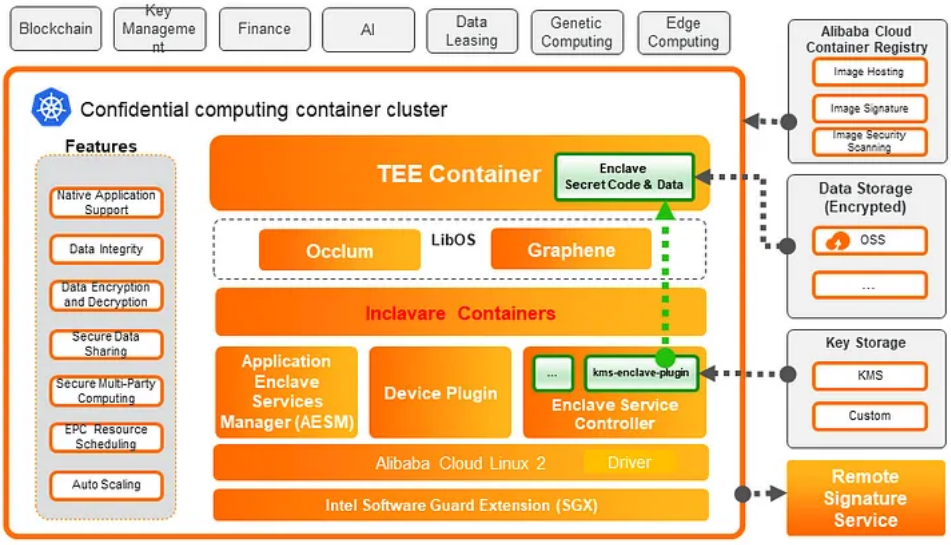

Figure 3.11: Alibaba Cloud product for CC - ACK-TEE [9].

Attestation with Alibaba Cloud

Confidential container solutions such as Inclavare Containers and Confidential Containers based on HW-TEE (such as Intel SGX, Intel TDX, and AMD SEV) can offer confidentiality and integrity protection for sensitive data in use in a cloud-native deployment. The Confidential Computing Consortium specifies the RATS (Remote Attestation) reference architecture and advises that all remote attestation services adhere to it. It is illustrated in Fig 3.12.

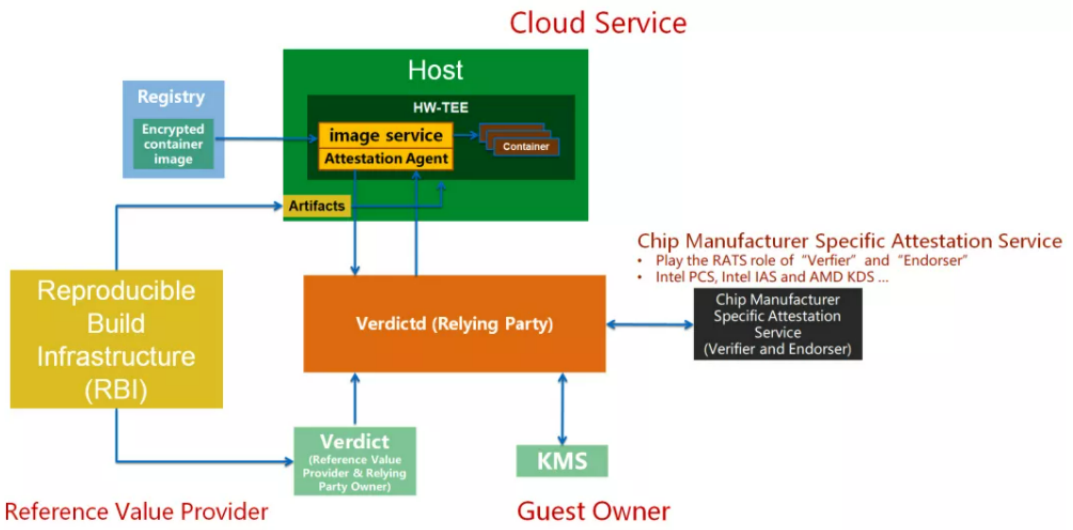

Figure 3.12: Alibaba Attestation EAA Architecture in accordance with the RATS Architecture [13].

Main Elements and Functions [13]:

- The component that operates inside the HW-TEE is known as the **Attestation-Agent (Attester)**. Its purpose is to acquire Evidence (HW-TEE signed measurement data from running applications).
- **Chip Manufacturer Specific Attestation Service (Endorser)**: A service supplied by the

chip manufacturer that runs on a public network. Its purpose is to validate the Evidence's signature to ensure that the measurement data is generated by the genuine HW-TEE.

- Verdict and Reproducible Build Infrastructure (Reference Value Provider): A service that operates in a user-trusted environment. Its purpose is to produce a reference value of the running program's measurement in the HW-TEE environment in order to establish if the running program's content in the HW-TEE environment is as expected.
- Verdictd: A service that runs in a user-trusted environment (Relying Party + Relying Party Owner + Verifier Owner). It is responsible for contacting the Chip Manufacturer's Specific Attestation Service and the Verdict and Reproducible Build Infrastructure to authenticate the received Evidence's signature and analyze its content in order to complete the remote attestation procedure.
- KMS: Key management service that runs in a user-trusted environment or public network to handle keys.

The precise documentation with Alibaba Cloud was welcoming but that also means the lack of research done previously. It checks all the boxes of Cloud technologies like Robustness, Scalability, auto-orchestration, etc. For our e-health data processing use case we have better suiting offerings from other CSPs. Hence, we chose not to move forward with Alibaba Cloud.

3.5 IBM Confidential Computing

IBM Secure Execution and IBM Protected Execution Facility (PEF) are two confidential computing architectures offered by IBM Systems. Since IBM Z15 and LinuxONE III, Secure Execution offers support for Secure Virtual Machines (SVMs) that run inside isolated TEEs. It uses trusted firmware, referred to as the Ultravisor, to carry out security-sensitive operations in order to boot up and run SVMs. The Ultravisor will use the decrypted sensitive data that tenants employing Secure Execution have embedded in the VM images to expose them to the SVMs running inside the TEEs. The public key associated with the embedded private key of the IBM Z or LinuxONE hardware is contained in the host key document, which is signed by the hardware vendor. Only the SVM running inside the TEE for the intended tenant is allowed access to the unencrypted data, as the Ultravisor is the only component with access to both the hardware private key and the data key. Using modifications to the IBM Power Instruction Set Architecture (ISA) that are supported by the majority of POWER9 and POWER10 processors, Secure Execution offers a VM-based TEE. Protected Execution Ultravisor (Ultravisor), a trusted firmware that shields the SVM execution and upholds the security assurances with the aid of changes to the CPU architectural design, is introduced by PEF to secure sensitive data and code. The VM is started by the hypervisor, which then uses the Enter Secure Mode (ESM) function to call the Ultravisor to switch to an SVM. The integrity information and a passphrase for the encrypted file system are decoded by the Ultravisor, which also does integrity checks and decrypts the payload attached to the SVM image. The access to the symmetric seed needed to verify the integrity and decode the payload is provided by the Ultravisor via the Trusted Platform Module (TPM). The HMAC key and symmetric key that are used to check the passphrase's integrity are generated by the Ultravisor if it has access to the symmetric seed.

3.6 Microsoft Azure

Azure is a cloud computing platform that offers a constantly growing range of services to assist you in creating solutions to achieve business objectives. Azure services range from basic web hosting for a company's online presence to completely virtualized PCs that one may use to execute their own unique software programs. Numerous cloud-based services, including remote storage, database hosting, and centralized account management, are offered by Azure. Azure also provides modern features like AI and the Internet of Things (IoT).

3.6.1 Azure - Confidential Computing support

Azure currently provides a wide range of capabilities for protecting data at rest, including client-side and server-side encryption. Azure also provides tools for encrypting data as it is being transmitted via secure protocols like TLS and HTTPS. Azure confidential computing reduces the requirement for confidence across various components of the compute cloud infrastructure, making it simpler to trust the cloud provider. Azure confidential computing reduces reliance on the hypervisor, host administrator, VM administrator, and host OS kernel.

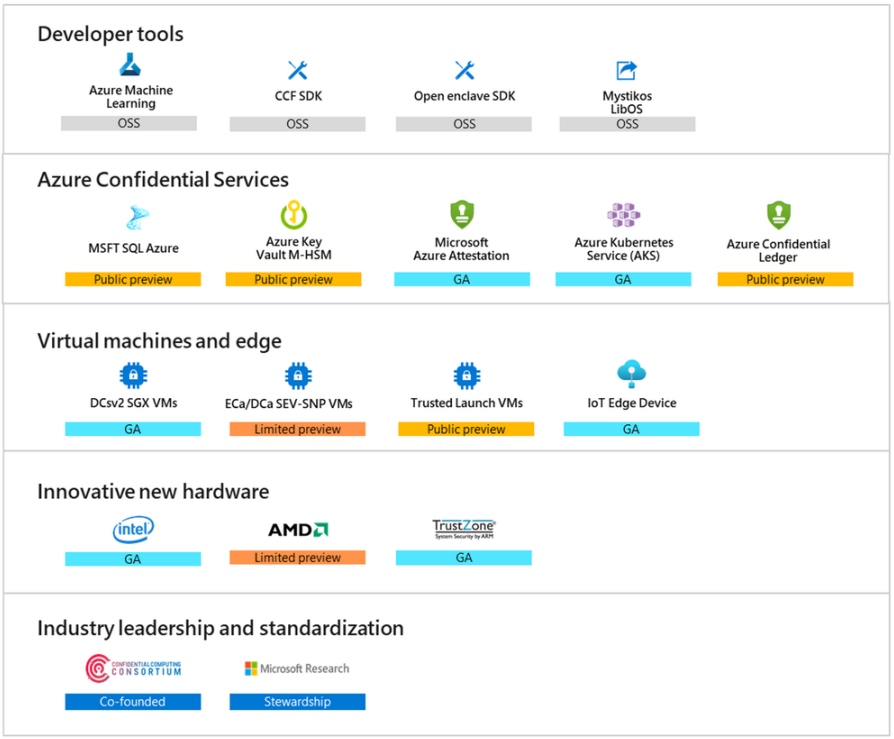

Figure 3.13: The Azure Confidential Computing technology stack [45].

Azure confidential computing can assist with [46]:

- **Prevent unauthorized access** - Run sensitive data through the cloud trusting that neither Azure nor anyone unauthorized can access it.
- **Meet regulatory compliance** - To comply with legal requirements for the protection of private information and the security of corporate intellectual property, migrate to the cloud while maintaining complete control over the data.

- Ensure secure and untrusted collaboration - To leverage broad data analytics and deeper insights, combine data from many businesses, including competitors, to address problems on an industry-wide scale.
- Isolate processing - A new generation of services that eliminate accountability for private data processing. Even the service provider is unable to access user data.

Azure also Offers the following services:

- Microsoft Azure Attestation - A remote attestation service for confirming the integrity of the binaries executing inside various Trusted Execution Environments (TEEs) and evaluating the trustworthiness of the TEEs.
- Azure Key Vault Managed HSM - A completely managed, extremely reliable, single-tenant, standards-compliant cloud service that lets you protect the cryptographic keys for your cloud applications using Hardware Security Modules (HSM) that have been validated to FIPS 140-2 Level 3.
- Trusted Hardware Identity Management - A service that manages certificate caching for all TEEs housed in Azure and offers trusted computing base (TCB) data to impose a minimal standard for attestation solutions.
- Trusted Launch - A virtual trusted platform module, and boot integrity monitoring are among the toughened security features of Trusted Launch, which is available across all Generation 2 VMs and guards against boot kits, rootkits, and kernel-level malware.
- Azure Confidential Ledger (ACL) - For the purpose of data transparency in multi-party scenarios, record keeping, auditing, and record keeping, ACL is a tamper-proof register for storing sensitive information. It provides Write-Once-Read-Many guarantees that prevent data from being altered or erased. The Microsoft Research Product[47] is the foundation of the service.
- Azure IoT Edge - Supports private applications that run on an Internet of Things (IoT) device in secure enclaves. Because IoT devices are physically accessible to criminals, they are frequently subject to manipulation and forgery. By securing access to data that is taken by and stored inside the device itself before it streams it to the cloud, confidential IoT Edge devices offer trust and integrity at the edge.
- Always Encrypted with secure enclaves in Azure SQL - By conducting SQL queries directly inside a TEE, sensitive data is isolated, and hence protected from malware and high-level unauthorized users.

The following compute resources use these technologies from Azure Computational Computing:

- VMs with Intel SGX application enclaves - for the creation of hardware-based enclaves, Azure offers the DCsv2, DCsv3, and DCdsv3 series based on Intel SGX technology. To safeguard your application's data and running code, you can create secure enclave-based apps that run in a number of virtual machines (VMs).
- App-enclave aware containers - operating on the Azure Kubernetes Service (AKS) platform from Azure. In order to establish separate enclave environments on the nodes between each container application, confidential computing nodes on AKS use Intel SGX.

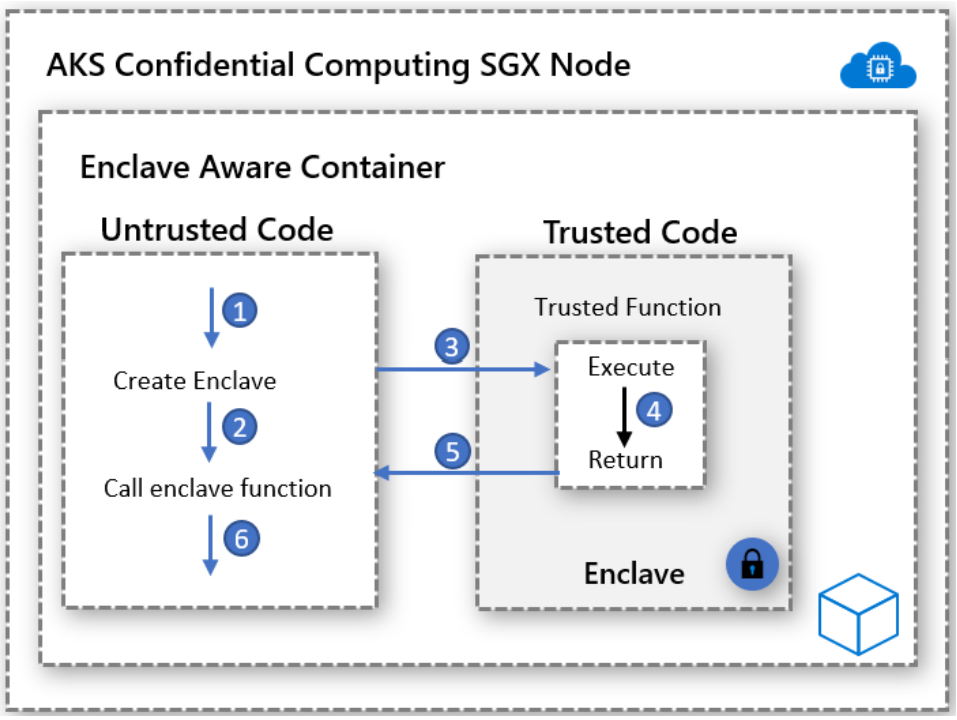

Figure 3.14: AKS CC SGX node [48].

- Lift-and-shift of current workloads is possible with confidential VMs built on AMD SEV-SNP technology, which also provides VM-level security to shield data from the cloud operator.
- Confidential Inference ONNX Runtime - a Machine Learning (ML) inference server that limits access to the inferencing request and its related response for the ML hosting party.

Depending on the use case, solutions can be designed using technologies like secure enclaves and confidential virtual machines.

- Confidential VMs built on AMD SEV-SNP technology can make it easy for existing apps without access to the source code to connect to the Azure confidential computing platform.
- Secure application enclave technology is useful for sophisticated workloads that contain proprietary code to protect from any trust vector. Intel SGX is used to protect data and programs executing in a hardware-encrypted memory region. To communicate with an acknowledged safe enclave, these apps often need open-source frameworks.
- For a balanced approach to confidentiality, a good solution may be using containerized solutions which are operating on secure containers enabled in Azure Kubernetes Service (AKS). In many cases, it is possible to bundle and deploy already existing software in containers with few modifications while maintaining complete security isolation from the cloud service provider and administrators.

Depending on the use case, one can choose the optimal VM for them based on their desired security posture from a variety of virtual machines offered by Azure for IaaS workloads including confidential computing. Figure 3.16 depicts the ẗrust ladderöf the security posture that clients might anticipate from these IaaS providers.

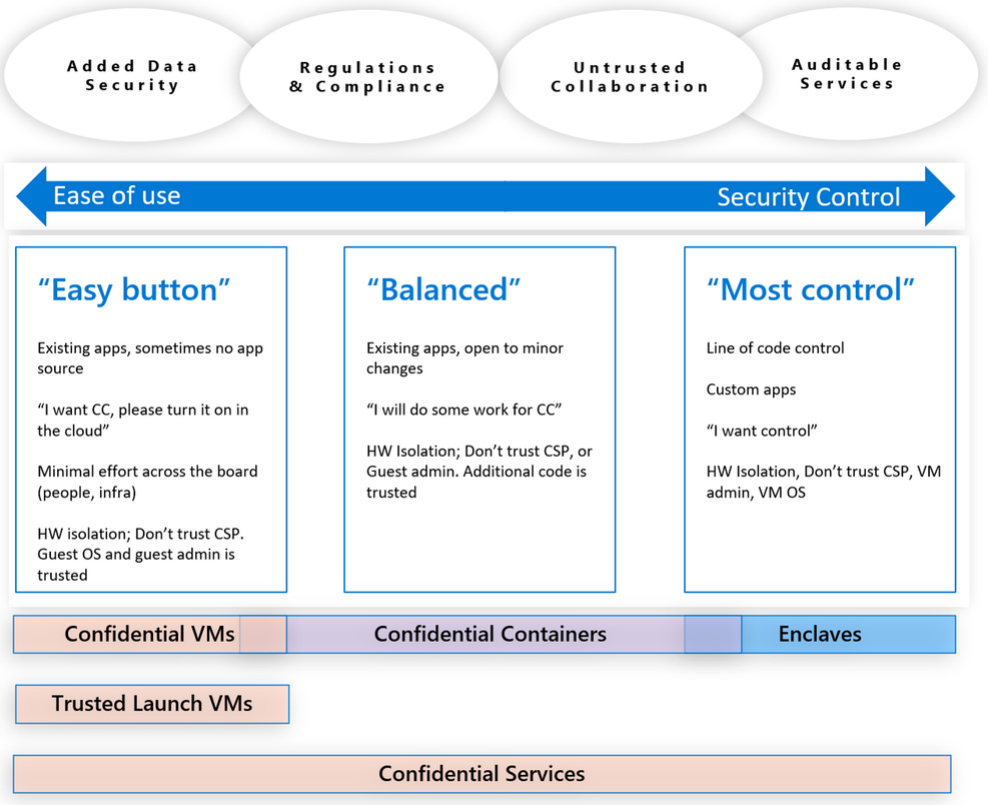

Figure 3.15: Control vs Ease in Azure Confidential Compute stack [45].

3.6.2 Azure Confidential Virtual Machines (CVM)

There are two CPU flavors available when selecting a Confidential VM Stock Keeping Unit (SKU). Either you choose a CPU that supports AMD Secure Encrypted Virtualization - Secure Nested Paging or you choose one that supports Intel SGX. It all comes down to how much of a TCB you're willing to assume when choosing a SKU[1]. The trusted computing base expands as we run more code inside of the trusted execution environment.

The hardware, firmware, and software elements of a system that create a secure environment are collectively referred to as the trusted computing base (TCB). The "critical" parts of the TCB are those parts. The security of the entire system may be at risk if one element inside the TCB is compromised. A lower TCB indicates more security [46]. Both suppliers can offer confidential computing capabilities because they both have a similar set of CPU features. Even while both systems enable the creation of TEEs, their applications are very diverse [51].

In a recent announcement [52], Azure has released in preview its DCesv5-series and ECesv5-series. These include 4th Gen Intel Xeon Scalable CPUs and Intel Trust Domain Extensions (TDX). Organizations can easily move sensitive workloads to the cloud using these VMs without having to make any code changes. Data integrity and confidentiality are guaranteed by Azure's Confidential VM family, which offers extensive business compliance and security measures. Though the ECesv5 series offers up to 64 vCPUs and RAM that spans from 8 to 512 GiBs, the DCesv5 series gives up to 96 vCPUs. Performance on compute-intensive tasks is improved by Intel TDX, and Azure intends to further optimize and adjust these virtual machines. The way these machines are named follows the following conven-

[1] represents a Stock Keeping Unit (SKU) for a product that may be purchased. These stand in for the various product shapes.

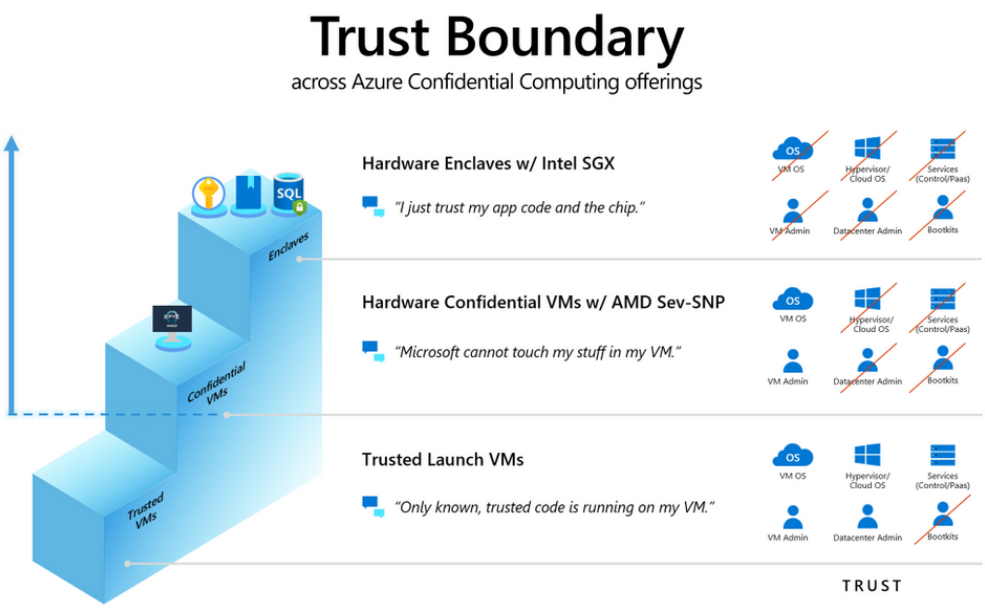

Figure 3.16: Trust boundary across Azure confidential computing services. [49].

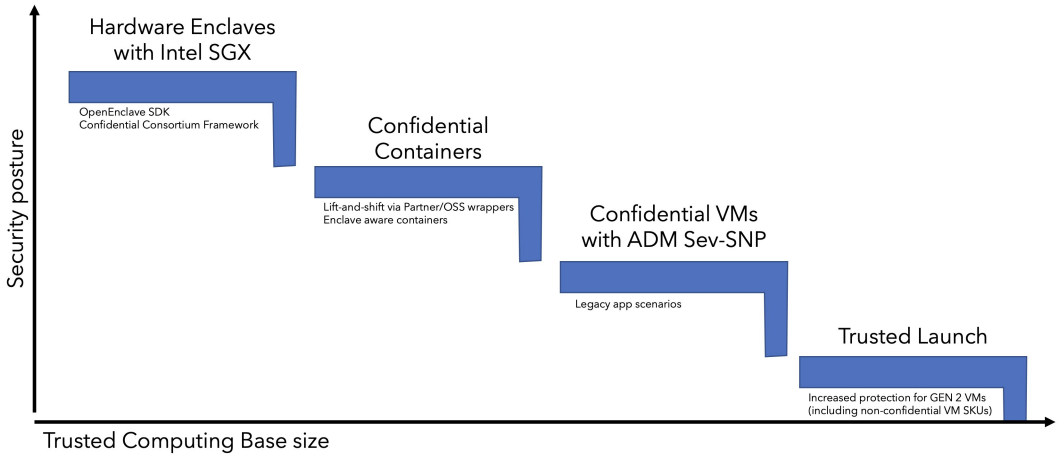

Figure 3.17: Security posture vs TCB size in Azure CC offerings [50].

tion: Standard - recommended tier, D – General purpose compute, C – Confidential, 2 – VM Size, a – AMD-based processor, d – Diskfull (local temp disk is present), s – Premium Storage capable, and v5 – version.

Azure Zero Trust Policy

Azure has a Zero Trust Policy. For business, technology, and security teams striving to safeguard everything as it is and as it could be, Zero trust is essential. Security professionals are on a continual journey, but getting there starts with easy first actions, a persistent feeling of urgency, and continued iterative improvements. Azure has created a Zero Trust architecture highlighting its importance for integrating threat protection, threat intelligence, automation, and policy enforcement. These integrated components use telemetry from all pillars to act on real-time signals to influence decisions as shown in 3.19. Its three primary pillars are as follows [53]:

- **Verify explicitly** - always authenticate and authorize depending on all information that is available, such as the identity of the user, their location, the health of their device,

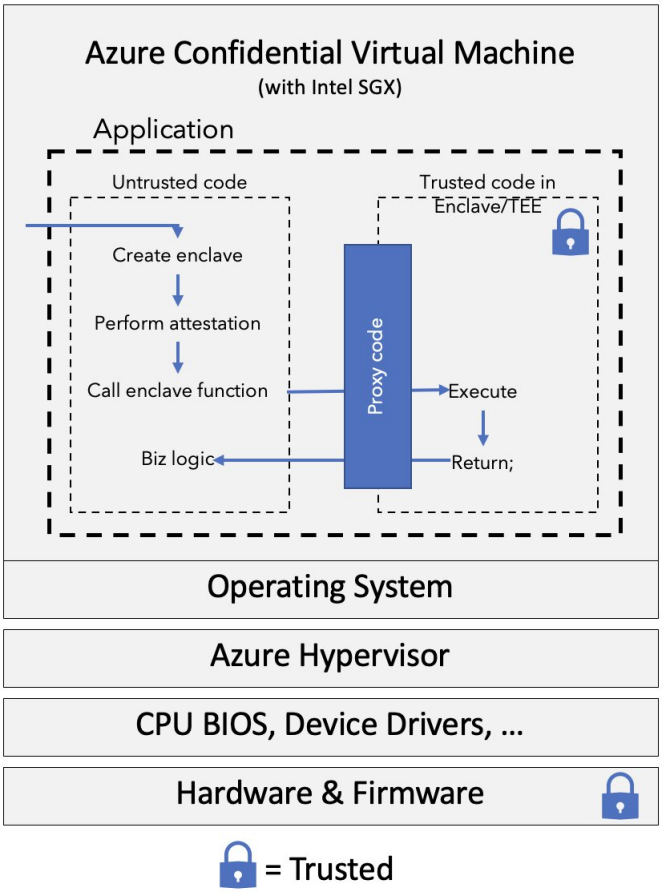

Figure 3.18: Azure Confidential VMs [51].

the burden they are putting on it, the type of data it contains, and any anomalies.

- Use least-privilege access - To help secure data and boost productivity, employ least-privilege access to restrict user access with just-in-time and just-enough access, risk-based adaptive policies, and data protection.
- Assume a breach has occurred and utilize analytics to get visibility, identify risks, and strengthen defenses. Verify end-to-end encryption.

Confidential Consortium Framework (CCF)

With a focus on multi-party computing and data, the Confidential Consortium Framework (CCF) is an open-source framework for creating a new category of safe, readily available, and fast applications [47]. CCF offers enterprise-ready multiparty systems by using the strength of trusted execution environments (TEE, or enclave), decentralized systems ideas, and cryptography. Web technologies provide the foundation of CCF, and clients communicate with JavaScript CCF apps over HTTPS. A CCF network is highly accessible and decentralized [47].

A CCF network is made up of many Intel SGX-powered nodes that are all operated by Operators as shown in Figure 3.20. Every node runs the identical JavaScript or C++ program, which is activated via HTTP commands sent by trusted Users over TLS. The Key-Value Store is a group of maps that the application defines. These maps can be either private (encrypted in the ledger) or public (integrity-protected and viewable by anybody with access to the ledger). Before being implemented, changes to the Key-Value Store must be approved by at least a

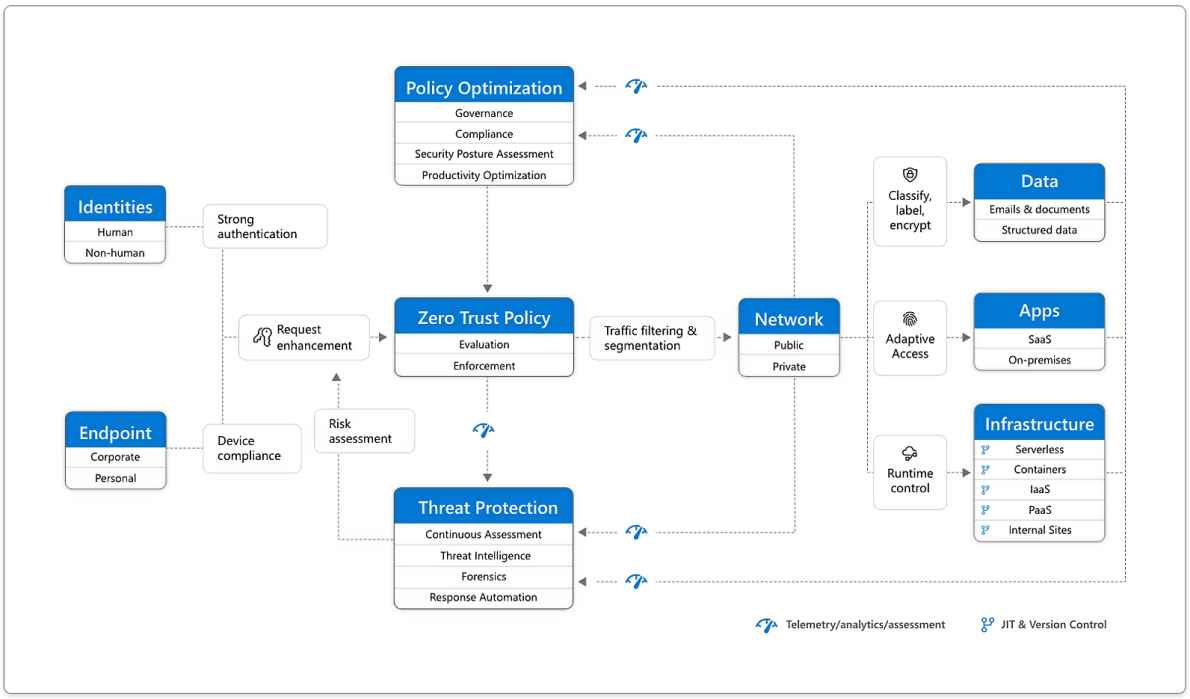

Figure 3.19: Azure Zero Trust Model [53].

majority of nodes [47]. It is simple to limit which maps (and entries in those maps) a user is allowed to read from or write to because every application endpoint has access to the identity of the user who initiated it. Each network node records all updates to the Key-Value Store to disk in an encrypted log that is decentralized and audited.

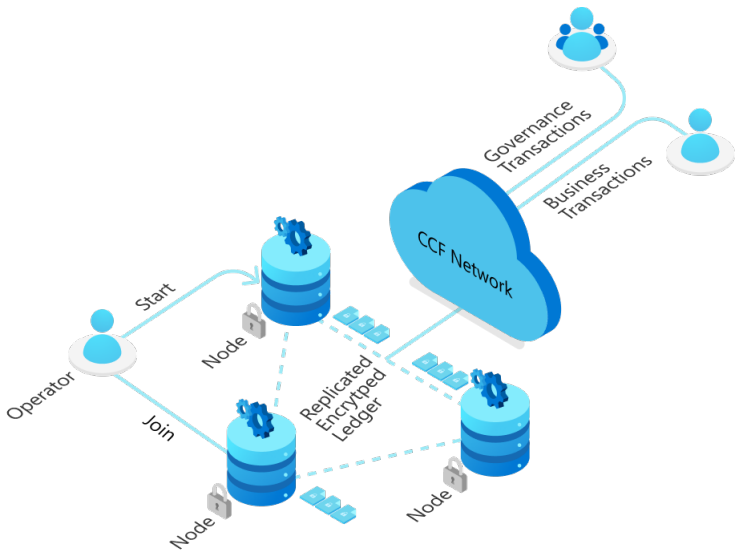

Figure 3.20: CCF Overview [47].

A group of Members oversees the CCF network. Members are required to abide by a set of rules as specified by the scriptable Constitution, which is stored in the ledger itself. Members are able to propose changes to the Key-Value Store's current status. Members can decide, for instance, whether to add a new member to the consortium or whether to allow a new trusted user to submit requests to the application [47]. The GitHub repository with more details can be found at [54].

Till now, Azure has the most advanced support for Confidential Computing as compared

to any other CSP we have researched. It has three different offerings that users can choose from according to the ease of use vs. modifications needed according to Fig. 3.15. There are all the Cloud computing properties available like Scalability, robustness, etc. As this is quite comprehensive, we will be going over more of this in the implementation of these offerings in Chapter 6.

3.7 OTC - Open Telekom Cloud

The German telecommunications firm Deutsche Telekom's Open Telekom Cloud is a large-scale, public OpenStack-powered platform that is supported and run by T-Systems across Europe. It was created with ease, security, compliance, affordability, and openness in mind. The cloud provider is built on OpenStack, an open-source platform that can lessen cloud providers' dependence on certain vendors. Electricity used to power the data centers comes only from renewable resources [55]. With geographically redundant data centers in Germany and the Netherlands and strict adherence to the European General Data Protection Regulation (GDPR), the Open Telekom Cloud satisfies the highest standards for data protection and security. Companies may be assured that their initiatives are in the finest hands because all data is kept in the EU or Germany.

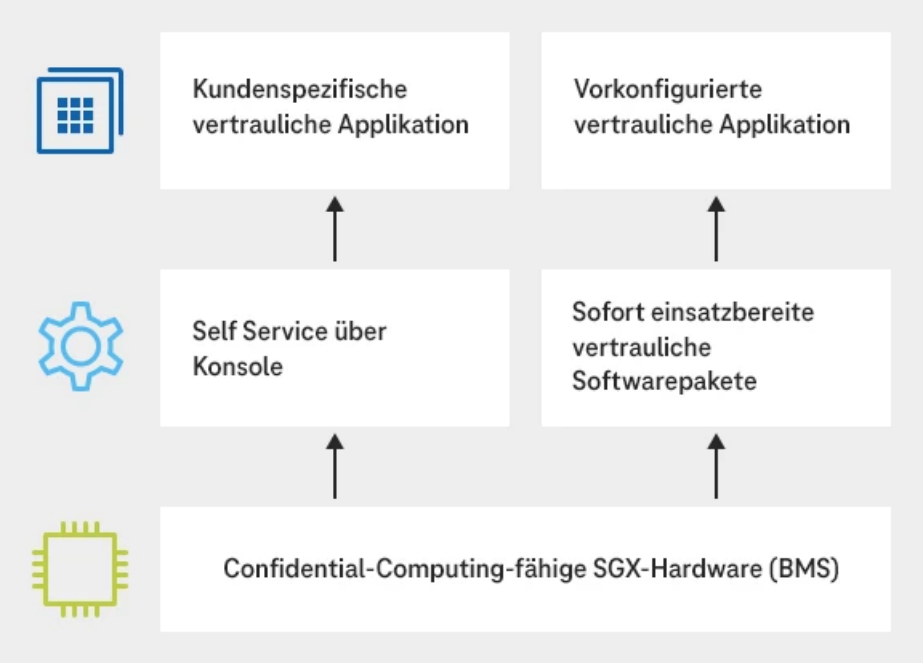

Figure 3.21: Open Telekom Cloud [56].

3.7.1 Open Telekom Cloud - CC support

Companies use encryption as part of their security strategies, but processing data requires decryption. Following the Privacy Shield and Europe's push for data sovereignty, this has sparked discussions. Companies that run sensitive data or workloads in public clouds must take additional technological security precautions, according to regulatory authorities in regulated industries. Confidential Computing ensures that sensitive data/workloads can be processed in encrypted form in a specially protected area, an enclave. This enclave is provided on a server that is also physically isolated, and the hardware used must be capable of confidential computing. The Open Telekom Cloud introduced Intel processors capable of using

Intel SGX as the basis for Confidential Computing. Businesses can choose a pre-configured (Bare Metal Server) BMS on the console if they want to employ confidential computing. This is additionally accessible in an elastic form, or on demand. A specialized partner of the Open Telekom Cloud can also be contacted for additional services in this area. This provides predefined options for using, for instance, TensorFlow, PyTorch, Apache Spark, MongoDB, Redis, and Maria DB [56].

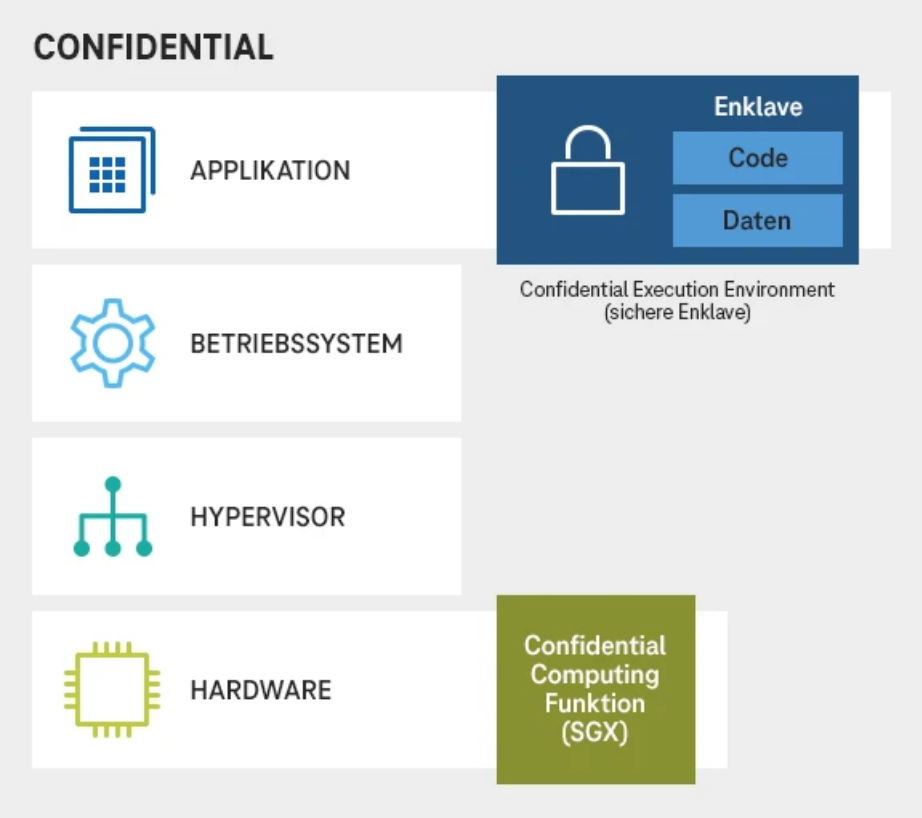

Figure 3.22: Open Telekom Cloud main Architecture [56].

3.7.2 Open Telekom Cloud (OTC)- Bare Metal Server (BMS)

Hypervisors and virtualization are absent from bare metal servers, which give users the most freedom to create their own systems because the computing resources are simply outfitted with a host operating system. On the basis of their own virtualization technology, they can create unique flavors. Without virtualization, bare metal servers can also be employed. Because they lack a hypervisor, they provide more reliable performance than virtual machines, which makes them the perfect choice for big data analytics. Additionally, bare metal servers provide better software license terms than traditional servers do. Open Telekom Cloud's Confidential Computing service is also built on a bare metal server (physical.i7n.28xlarge.4) [57].

Motives for utilizing BMS on the Open Telekom Cloud:

- **Legal compliance** - Allocated resources operate in a GDPR-compliant setting and satisfy all European standards for running secure workloads with scalable cloud alternatives. Authorities outside of Europe have no access.
- **Enhanced performance** - Dedicated computing resources can be used with BMS without extra hypervisor overhead. This custom hardware provides a higher level of safety

and efficiency while eliminating the "noisy neighbor" effect, which is when other users' use of the assigned resources has a detrimental impact on their performance.

- High flexibility - The services can be quickly implemented and are customized to one's needs.

Key features of BMS in Open Telekom Cloud:

- High integration with services - Cloud Eye (CES), Elastic Volume Service (EVS), Scalable File Service (SFS), Virtual Private Cloud (VPC), Image Management Service (IMS), and Volume Backup Service (VBS), etc.
- Security and isolation - Physical resources can be separated using the BMS service so that other tenants cannot affect them.
- Fast network - BMSs can connect at high speeds using InfiniBand at speeds up to 100Gbps.
- Easy billing options - Elastic (paid by the hour), Reserved (discounted monthly price for sustained use), and Reserved advance (additional discounts through advance payment) are the three pricing tiers available for the BMS Service. The operating system license fees have already been paid.
- Bring your own license (BYOL) - By making use of pre-existing licenses like RHEL, SUSE (SLES), Microsoft Office, etc., the BYOL license type lowers expenses.

From the available research on OTC and its attestation capabilities, it looks like OTC also checks all the boxes. However, as it does not have any capability of offering a Confidential Virtual Machine, we might have to make one ourselves on top of the BMS offering. From the initial impressions, the BMS offering of OTC is quite similar to the one from OVHcloud. Its implementation was easily available as this is an in-house offering of the Deutsche Telekom AG group.

4 Requirements and Related Work

4.1 Basic Research and Requirements

Almost all countries struggle to offer inexpensive healthcare that is of better quality and convenient to receive. There is an increasing demand for a safe and affordable e-health system in the healthcare industry. It encourages health managers to develop and implement cutting-edge healthcare services in the healthcare industry to track disease trends as well as the state of public health [58]. Several studies on cloud-based medical apps state that the cloud is the best way to meet healthcare needs [59]. Moreover, the cloud offers robust processing, effective storage, and deep analytics on healthcare data [60]. The use of cloud computing resources in the healthcare industry is the main topic of numerous researchers [61]. They model the potential for developing a cutting-edge healthcare system that makes use of the most recent cloud computing services provided by several cloud service providers [62, 63, 64]. In [65] the author Kuo M covered the opportunities and difficulties associated with integrating cloud computing into the healthcare industry. Further research on the topic provides cloud computing service models that can serve various medical services in the healthcare sector [66]. A cloud-based system design was presented by the author to help mid-sized hospitals administer their services at a reasonable cost [67]. The difficulties in integrating cloud computing in the medical industry are listed by the author Changming Chen in [68]. Leading cloud service providers are interested in providing state-of-the-art cloud services to manage the data flow in various healthcare system stages.

For the final product, it important we have a confidential computing enabled system stack on cloud. That could be an IaaS (Infrastructure-as-a-Service) offering or a PaaS (Platform-as-a-Service) offering. It is essential to have attestation capabilities in the selected product. The general cloud stack looks like this:

CSPs' offers specific to Healthcare

To keep up with innovations in the field of healthcare, CSPs create new service offerings. To manage big data, machine learning, and related analytics for improved insights into healthcare data, Google Cloud Platform (GCP) has expertise in providing healthcare Application Programming Interfaces (APIs). Healthcare firms have a fantastic opportunity to manage their data safely with the help of Amazon Simple Storage Service (S3) for storing and Amazon Elastic Compute Cloud (EC2) for computing [69]. Healthcare data management services are offered in a variety of ways by Microsoft Azure. Fast Healthcare Interoperability Resource (FHIR) is supported by Azure's most recent services to manage healthcare data in the cloud.

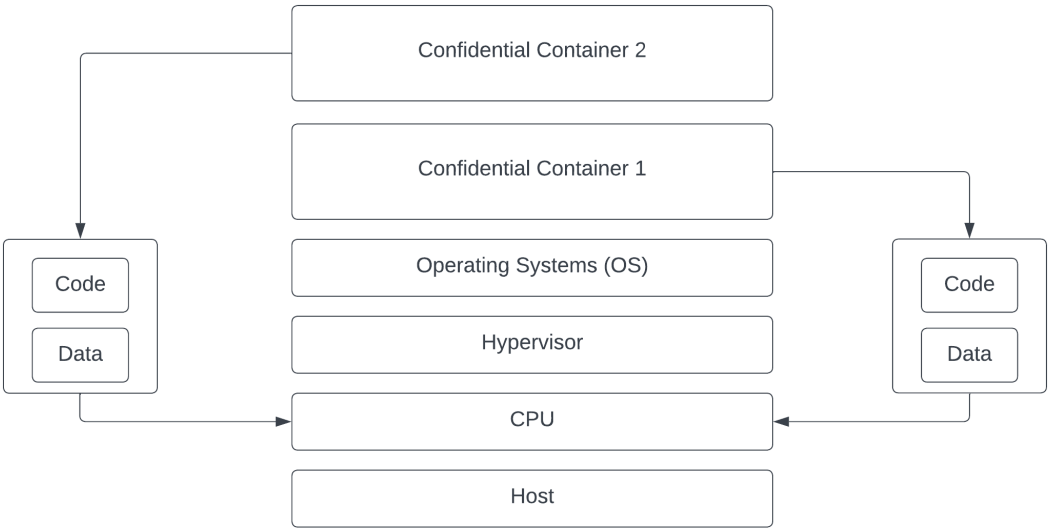

Figure 4.1: The basic Architecture sketch.

To leverage these services, any healthcare institution must first build an appropriate architecture. To obtain certain business values and insights, the healthcare data that has been stored in the cloud in the desired format needs to be processed and examined utilizing these services.

The CSP can only be trusted for the Availability of the guest. Attestation- overview and how it's different with SEV-SNP (Secure Nested Paging) is shown in Fig. 4.2.

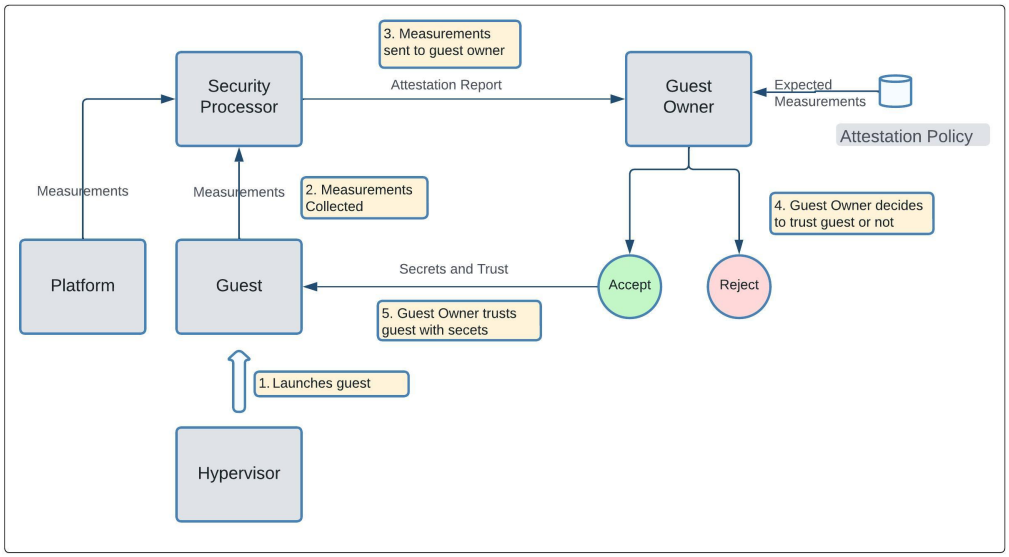

Figure 4.2: Attestation Overview [29].

4.2 Frameworks/Adaptations

The following frameworks and adaptations take the software stack to the new generations. They extend the simple functionality of SGX and build on top of it, like in the case of Graphene. OR, in the case of Scone and Fortanix, a new product from the ground up. These solutions

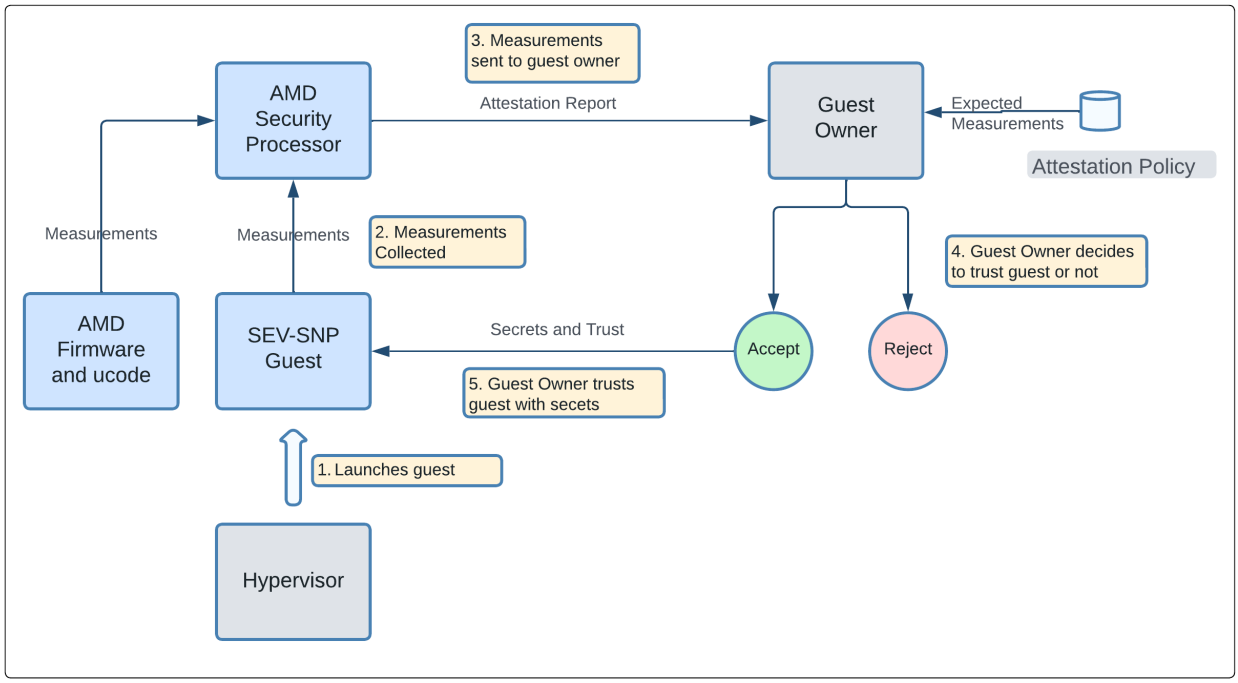

Figure 4.3: Attestation Overview - SEV-SNP[29].

come in a role and can be deployed when we need managed services on our cloud platform. Or, if we need to 'enable' confidential computing functionality on our cloud resource, which is otherwise not available natively. They, however, need the Intel SGX or the AMD SEV to function. Having a TEE is the very basis of how Confidential Computing works.

4.2.1 Graphene SGX

What's Graphene?

A single program can be executed on Graphene, a lightweight library OS with little system requirements. With advantages similar to those of running an entire OS in a virtual machine, including guest customization, ease of porting to multiple OSes, and process migration, Graphene can execute programs in a closed environment. On any platform, Graphene supports native, unmodified Linux binaries. Graphene now operates on Linux platforms and Intel SGX enclaves. There is a strong desire to isolate the entire application from the rest of the infrastructure in untrusted cloud and edge deployments. This lïft and shiftpäradigm for transferring unaltered apps into Confidential Computing with Intel SGX is supported by graphene. With little effort in porting, graphene can shield programs from a hostile system stack. In addition, Graphene fully supports SGX Attestation, protected files, multi-processing with encrypted IPC, and the upstreamed SGX driver for Linux. With full compatibility with automated Docker container integration utilizing Graphene Shielded Containers (GSC), the developers have added lots of performance optimizations for SGX and provided tools to more easily deploy in cloud settings.

Graphene SGX and it's architecture

Graphene-SGX is a simple, open-source tool for quickly bringing up existing apps on SGX and then iteratively adapting the code to improve SGX performance and security [20]. Intel

SGX adds hardware characteristics that enable applications to protect themselves from the host operating system, hypervisor, BIOS, and other software. Enclave characteristics include confidentiality and integrity protection, control flow restriction into well-defined entry points, memory integrity verification at startup, and remote attestation. Because consumers may not entirely trust the cloud provider, SGX is especially appealing in cloud computing. However, programs do not just workön SGX since SGX enforces enclave code constraints that necessitate application changes or a layer of indirection. The authors in [20] shows how to use a library OS to quickly deploy apps in SGX while receiving immediate security benefits without incurring debilitating performance costs or TCB bloat. The performance overheads in Graphene-SGX, a port of the Graphene library OS to SGX, are equivalent to the range of overheads reported in SCONE. The primary way to reduce TCB is to compile out unnecessary library functionality or to further split a program into numerous enclaves with fewer OS needs. Graphene's goal is to quickly launch rich applications on SGX and then allow developers to optimize code or reduce the TCB as required. Graphene-SGX runs unchanged Linux binaries on SGX, and users simply need to specify features and sign the configuration cryptographically. Graphene-SGX can also be used to speed SGX research.

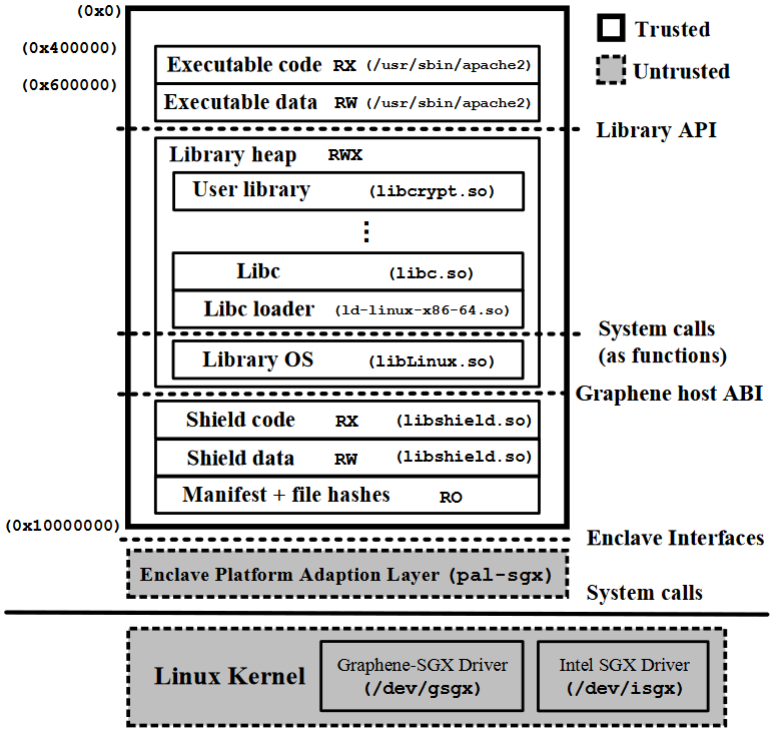

Figure 4.4: Graphene SGX Architecture [20].

Intel - Project Amber

Announced in 2022, this planned service codenamed Project Amber [70], is a new method for independent third-party attestation. It is a SaaS-based trust authority that allows remote verification of a compute asset's trustworthiness based on attestation and policy.

Project Amber initially validates the trustworthiness of Intel trusted execution environments (TEEs), but the concept extends to far broader device validation, including IPUs, GPUs, platform roots of trust, and beyond. Amber is designed as a cloud-native microservice platform that runs on a managed Kubernetes service, with appropriate abstractions on various cloud infrastructure platforms, on-premises, and edge locations.

Key Advantages:

- Independent - Trustworthiness verification by an independent authority provides customers with improved confidence, and a solid security basis for confidential computing, and opens up new applications in AI, multi-party computation, and federated learning.
- Scalable Cloud - agnostic SaaS and multi-cloud workload support: Project Amber enables enterprises to scale and migrate workloads more securely across a wider variety of edge, on-premise, and cloud environments – all while improving data and intellectual property protection.
- Turnkey - It relieves businesses of the need to construct and operate a sophisticated and costly attestation system.

Project Amber is Intel's initial step toward developing a new multi-cloud, multi-TEE service for third-party attestation, and it will accelerate the industry's adoption of confidential computing. Amber 1.0 Pilot enables secure compute workloads deployed as bare metal containers, virtual machines (VMs), and containers operating in virtual machines using Intel TEEs. Support for other non-Intel TEEs on the market will be extended in 2023.

4.2.2 SCONE - Secure CONtainer Environment

With the SCONE confidential computing platform, it is possible to execute services and applications with consistent encryption so that neither the data nor the code is ever visible in plain text, not even by root users. The only thing that can access the unencrypted data and code is the application code itself. Input encryption, service/application execution in encrypted memory on an untrusted host, transparent output encryption, and sending the encrypted output back to the client are all made simpler by SCONE. SCONE enables the execution of private apps inside containers that are part of a Kubernetes cluster. SCONE also allows for the execution of private software on bare metal hosts as well as inside virtual machines (such as those running Windows 10). Every popular programming language is supported by SCONE. Additionally, it supports air-gapped systems that use both SGXv1 and SGXv2 protocols. On contemporary SGX-capable CPUs, SCONE-based apps can use up to 32GB of memory. According to Intel's SGX standard changes, future CPUs will allow even larger enclaves, and SCONE will support practically infinite memory-size applications on these CPUs.

Programs linked with glibc (the default for Ubuntu, Centos, and RHEL) and musl (the default for Alpine Linux and hence, many container images) are both supported by SCONE for execution inside of enclaves (at use encryption). SCONE supports both static and dynamic linking, as well as all widely used programming languages. It also supports support a cross-compiler for application development, which is how it is advised to create private applications.

SCONE enables the constant encryption of data, communications, code, and main memory. To accomplish this, SCONE must confirm that the anticipated application code is being executed in a trusted environment on a potentially unsafe host. SCONE's Configuration and Attestation Service (CAS) can assist with encrypting input and output data on a local computer. Multiple stakeholders (confidential multiparty computation) are supported by SCONE, even if they are not necessarily trustworthy of one another. This allows for the protection of each party's intellectual property. Since clients can confirm that the services are in the proper state, some of the services, like SCONE CAS, might be run by stakeholders who are not always seen as trustworthy.

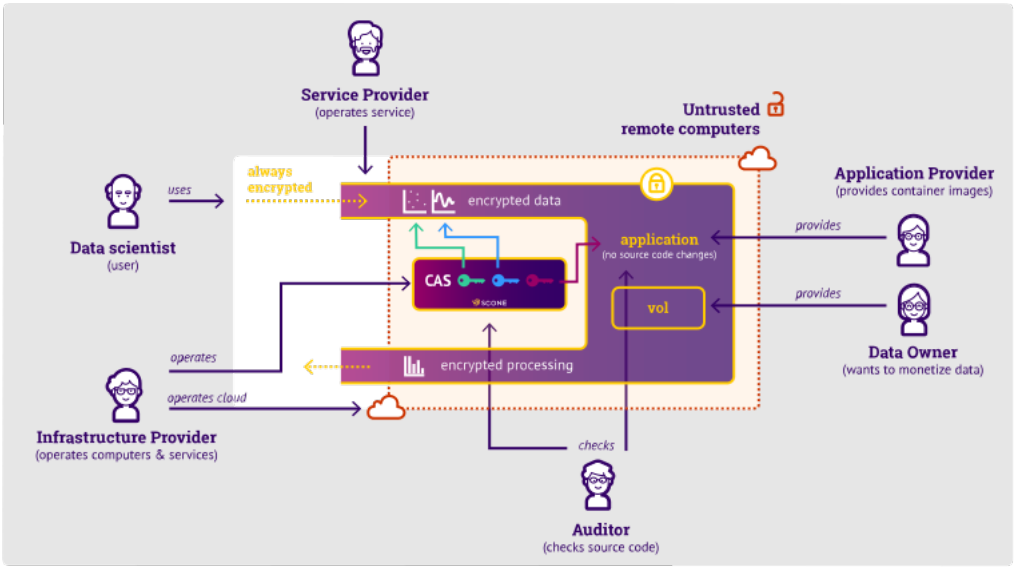

Figure 4.5: SCONE Overview.

SCONE - Shortcomings

Like Graphene-SGX [20], SCONE [71] provides a Library OS with syscall functionality and a protective layer for host services. Docker containers can be integrated with secure SGX enclaves using SCONE. But like other solutions, SCONE endures a number of problems brought on by Intel SGX, particularly its rigid memory management of SGX enclaves (allocated at system boot), which forces programmers to precisely implement SGX-specific multithreading by spawning threads in the host process that all enter the enclave. Additionally, because SCONE uses a user-space threading model, it cannot handle some system calls like exec or fork, which requires changes in many legacy applications. For an existing application, this could be very time-consuming to 'sconify' the whole application. There is, however, research going on how to make this process both easy to implement and port.

4.2.3 Fortanix

Fortanix is a founding member of the Confidential Computing Consortium, along with Google, Intel, and Microsoft. Confidential Computing Manager (CCM) from Fortanix safeguards data in use via a trusted execution environment (TEE) or secure enclave, which runs data totally encrypted in memory, isolated from the infrastructure. Data stays secure even if the infrastructure is hacked, lowering the chance of data leaks. Fortanix CCM streamlines enclave lifecycle management procedures across different public clouds and on-premises systems, including creation, deployment, monitoring, and auditing. Confidential computing transforms how clients protect sensitive data and manage important security rules including identity verification, data access control, and code attestation.

Fortanix Runtime Encryption(R) Platform is currently available as an IBM Cloud Data Shield service. This service runs on top of IBM Kubernetes Service (IKS), allowing applications to run as containerized services. Upon installation, IBM Cloud Data Shield launches the Confidential Computing Manager, enrolling worker nodes from the Kubernetes cluster in IKS. These nodes can be accessed via the web console, along with their SGX attestation information. A container conversion tool transforms Docker container images into SGX-capable images by inserting EnclaveOS and configuring parameters. Confidential Computing Manager can whitelist the changed container image, and the container can be deployed using the usual Kubernetes interface. Confidential Computing Manager validates the attestation and issues

the application with TLS certificates.

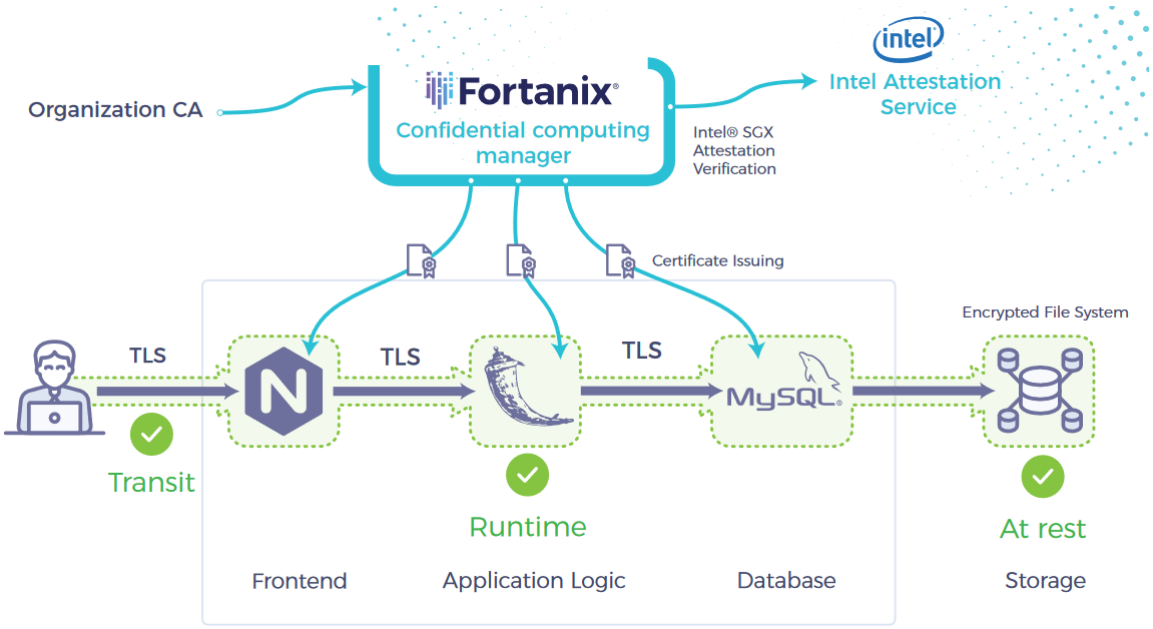

Figure 4.6: Fortanix Runtime Encryption used in an application [72].

These framworks could come in picture when we take on the BMS offerings from either of OVHcloud or from OTC. They can, of course be combined with the other Cloud Confidential VM offerings. Numerous combinations are hence, possible.

4.3 Existing Solutions - Healthcare and Confidential Computing

While researching the Literature already available in the field of e-health data processing, we came across a few intuitive solutions that are very efficient and give a good overview of the technology. The solutions combine the good parts and make a tech stack that resembles a final, secure, working IaaS or SaaS solution.

4.3.1 Azure - Healthcare application with CC stack

A very detailed and common use case is defined by Microsoft Azure's former Principal Product Manager, Gowda [73]. The solution offers a mechanism for a provider-hosted application to securely work with a hospital and a third-party diagnostic provider using confidential computing and containers. Azure Kubernetes Service (AKS) is used to host nodes for confidential computing. Trust is established with the diagnostic provider through Azure Attestation. The architecture protects the hospital patients' sensitive data by leveraging these Azure components, while the particular shared data is processed in the cloud. The diagnostic provider is then unable to access the hospital data. The provider-hosted application can benefit from sophisticated analytics thanks to this architecture. These insights are made available by the diagnostic provider as private computer services for ML programs. On a deeper dive, in simple terms, the use case can be summarized as follows:

1. A web portal is opened by a hospital employee in the area. The entire web app is a static website hosted on Azure Blob Storage.
2. The clerk inputs information into the hospital's website, which links to a web API built with Python Flask and developed by a well-known provider of medical platform soft-

ware. The patient data is protected by a confidential node in the SCONE confidential computing program. The SGX feature, which helps run the container in an enclave, is enabled on the AKS cluster in which SCONE runs. The Web API will show that the app code and sensitive data are isolated in a TEE and encrypted. The cleartext data and the application code are thus not accessible to anyone else, including logs, processes, or even humans.

3. The web app client for the hospital requests that an attestation service (Azure Attestation) validate this proof, and in return, it obtains a signed attestation token that other apps can use to confirm it.

4. In order to confirm that the data and app code have so far remained in a safe enclave, the Web API can pass along the attestation token if it needs additional components (such as a Redis cache) (read step 6 for verification).

5. Even remote services, like an ML model hosted by a third-party diagnostics provider, can be consumed via the Web API. It does so while continuing to transmit along any attestation tokens that serve as proof that the necessary enclaves are secure. Additionally, the Web API could try to get and validate attestation tokens for the infrastructure of the diagnostic vendor.

6. The medical platform's web API sends an attestation token, which the remote infrastructure accepts and verifies using a public certificate from the Azure Attestation service. It is almost certain that the enclave is secure and that neither the data nor the app code has been accessed outside of the enclave if the token is verified.

7. The diagnostics provider transmits the data into its own enclave in an ONNX runtime server because it is certain that it has not been exposed. The medical platform's private Web API app receives diagnosis results from an AI model once it has interpreted the medical imaging. The program can then interface with patient records and/or get in touch with other hospital employees from this point.

HTML, CSS, JavaScript, and image files are examples of static material that Azure Blob Storage serves straight from a storage container. A single solution called Azure Attestation allows for the remote verification of a platform's dependability. The integrity of the binaries that are used by the platform is additionally remotely verified by Azure Attestation. To build confidence with the private application, use Azure Attestation. Deploying a Kubernetes cluster is made easier with Azure Kubernetes Service (AKS). Confidential computing nodes are hosted on a particular virtual machine series that enables user-level programs to allocate exclusive memory regions, or "enclaves," to run delicate workloads on AKS under a hardware-based trusted execution environment (TEE). Enclave-aware containers or confidential containers can both be supported by confidential computing nodes. A Kubernetes cluster's Secure Container Environment (SCONE) allows for the running of private applications in containers. The SCONE platform is an independent software vendor (ISV) offering from Scontain which is an Azure Partner. Redis fits the use case here, as it is an open-source, in-memory data structure store. Confidential Inferencing the ML hosting party is prohibited from reading both the inferencing request and its matching response by the ONNX Runtime Server Enclave (ONNX RT - Enclave). This is how the components of Azure and others (SCONE, Redis) are fitting into this particular solution.

4.3.2 E-PIX - Record Linkage

A record linkage and uniform system-wide keying are needed to combine research data from many projects and studies and identify the relevant person for each one. It must be feasible

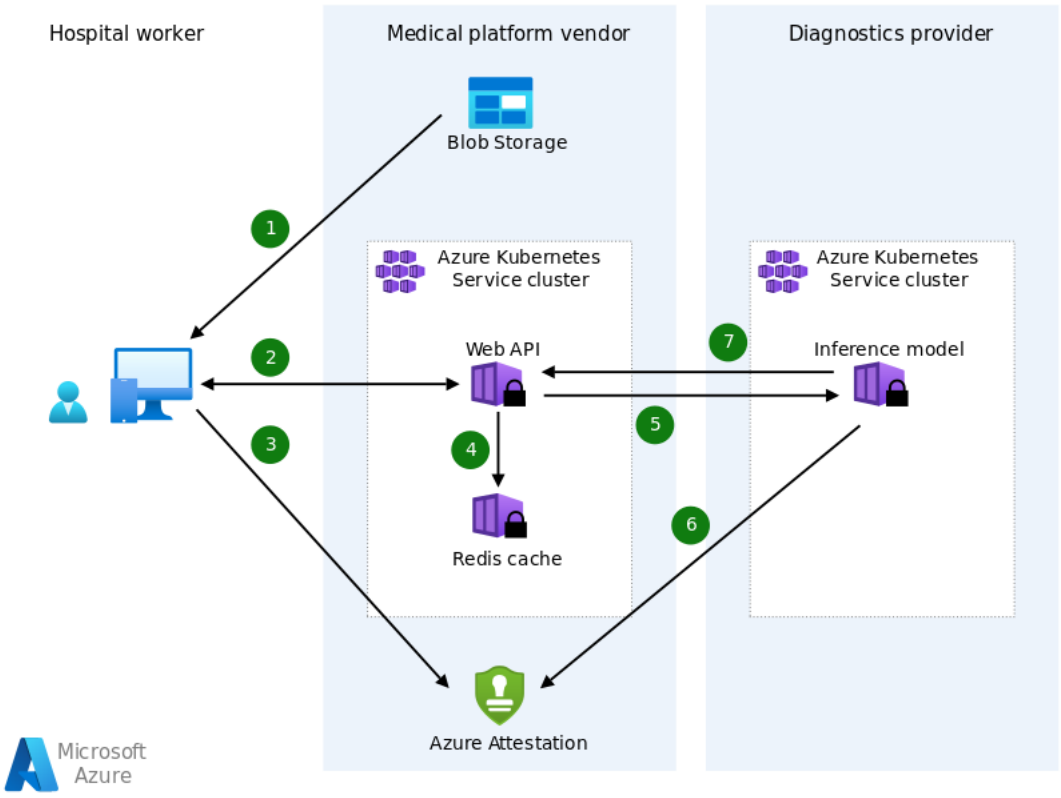

Figure 4.7: Architecture - Confidential computing on a healthcare platform <insert cite>.

to assign the unique local identifiers of the source systems (such as labs, study centers, etc.), in addition to managing personal identity data (IDAT). An error-tolerant and verifiable record linkage is necessary since IDAT may be incomplete or mistaken. As claimed, all of these tasks are taken on by the E-PIX [75].

The E-PIX [76] incorporates the idea of a master patient index (unique identification) and permits probabilistic record linking. E-PIX can handle a person's various IDATs (identities), enable the automatic detection of potential synonym errors (doubles), and help the resolution of these issues. Based on freely configurable parameters, Doppler detection is performed. Additionally, you have a choice of many pre-existing comparison algorithms or your own custom algorithm. Possible synonym errors are recorded and later fixed using E-PIX capabilities. Cross-site research initiatives demand extra security from the IDAT. By creating and comparing coded IDAT, the E-PIX provides a Privacy-Preserving Record Linkage (PPRL).

Frontend for the User - What a user can do:

- **Capture patient Data in a webpage format** - With a variety of demographic details, various contact information, and project-specific factors, patient data can be recorded and later on, even modified.
- **Find and remove redundant double entries** - Multiple entries for the same individual can be found using customizable methods. The E-PIX surface can be used to manually resolve these doubles or automatically.
- **Process lists** - The integration of E-PIX and other software packages is made easier by the adjustable import and export of Excel lists or CSV files.
- **Log events** - When matching people, the traceability of record-linking events is crucial. The log overview details matching outcomes as well as whether personal information

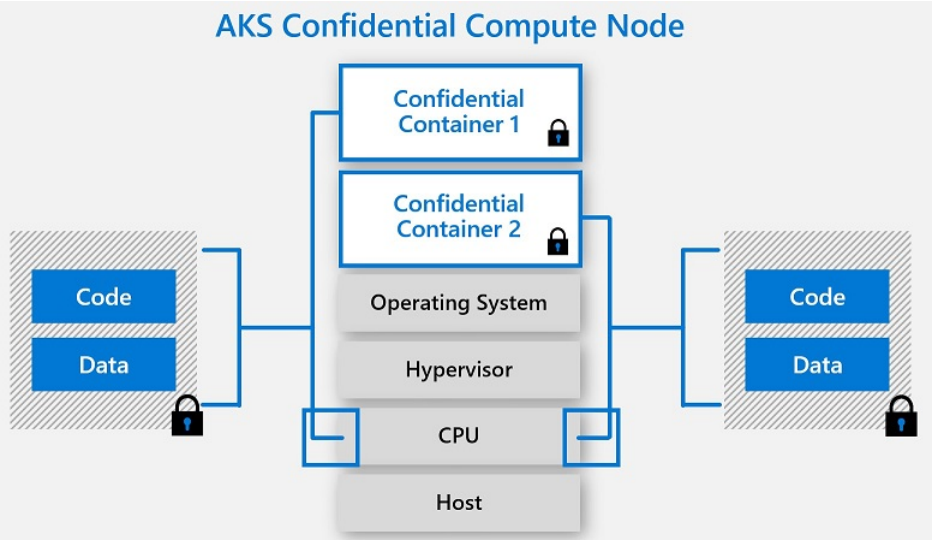

Figure 4.8: Azure Kubernetes Service (AKS) Confidential Compute node [74].

was updated, initially registered, or identities were added to already existing people.

Benefits at a glance:

- **Fast** - In a relatively short period of time, millions of data records are processed and verified for potential duplication.
- **Traceable** - The original data record may always be viewed because all data changes are historied.
- **Probabilistic linkage** - It is determined whether two people are linked based on programmable algorithms and threshold values.
- **Responsive** - You may work on your laptop or tablet in addition to the E-PIX because it has been designed for various screen sizes and gadgets.
- **Flexible** - To suit certain tasks, Doppler detection, plant detection, and many more techniques can be used. Consequently, it is possible to work on multiple projects at once.
- **Multilingual** - The help and user interfaces are entirely available in both German and English. At any time, users can choose the appropriate language.

What does the System do?

- Creation and management of a system-wide unique identifier using an index generator based on the concept of the Master Person Index.
- Merging of personal data from different source systems based on demographic information.
- Handling of erroneous/incomplete personal data.
- Support for recontacting using the integrated person management.
- Support for resolving potential matches using the concept of main and secondary identities.

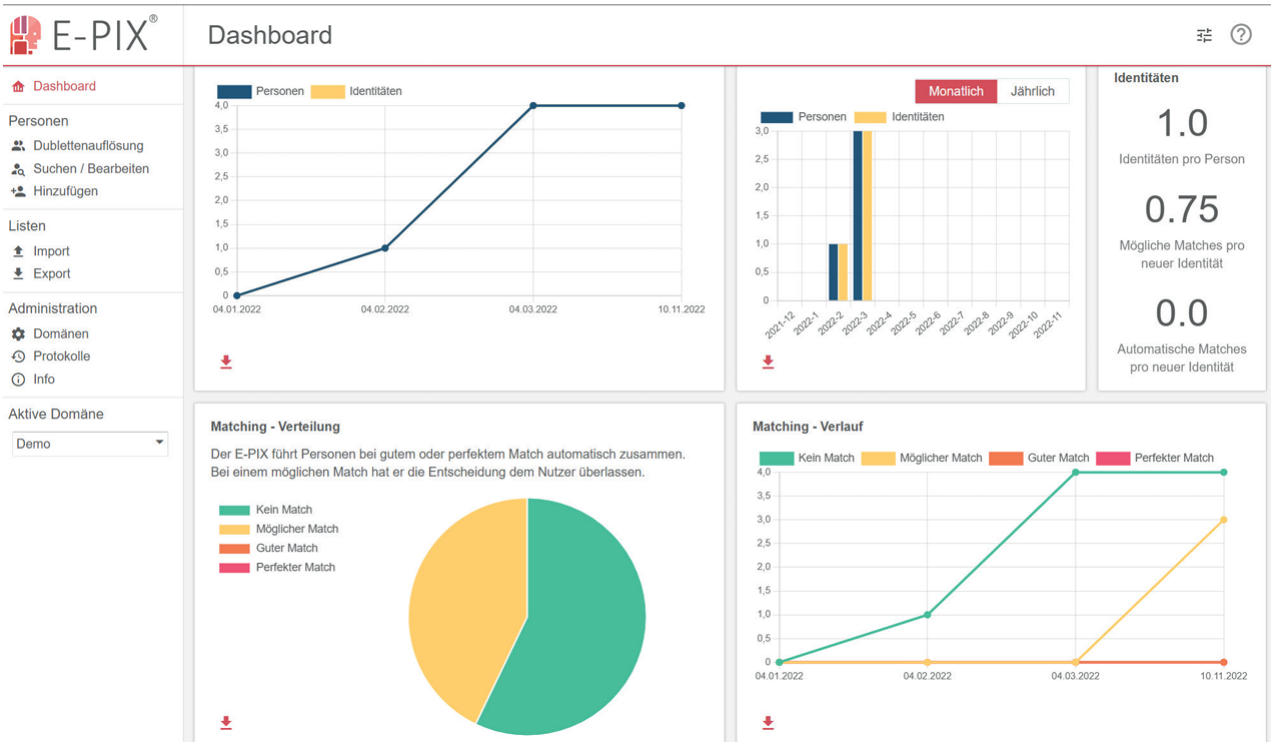

Figure 4.9: E-PIX Dashboard [75].

- Support of the IHE profiles PIX and PDQ (PIX is currently still without update notification).
- Logging of system processes and (critical) system decisions.
- Accelerated matching through caching: the database required for the matching process is kept completely in the cache and allows for example response times when creating or updating a person and a database of already 1. 000,000 persons in significantly less than 1 second.
- Easy operation through an intuitive graphical user interface.
- Sending of notifications in case of status changes to inform other systems.

4.3.3 Federated Learning e-health use case (Intel)

Federated learning [5] is the process of using many data sources (typically spread across various businesses or organizations) to train a single machine-learning model that is then applied separately to each data source. Based on its local data, the data host changes the existing model and transmits this update to a central server where it is aggregated. This avoids the bandwidth, security, and risk issues associated with sending significant amounts of sensitive or priceless data to a central source. It does, however, have a number of possible security flaws. The first is that there is no inherent protection for either the data or the model. The model can become 'poisoned' or corrupted, and the data could be seen or changed without permission. For a variety of potential use cases, such as training a model on patient data from multiple hospitals to develop better diagnostic models, rival banks cooperating to develop better anti-money laundering models, or retailers and commercial partners cooperating to develop more targeted offers (for instance, an airline and a credit

card company), this vulnerability is very difficult to exploit. Although there must be a mechanism to safeguard both the model and the sensitive data, there are enormous potential benefits in each of these scenarios.

Confidential Computing enables us to do this. The data set and the algorithm are both encrypted and more securely guarded. The data and the model are created to avoid exposure to potential tampering, with the data analysis happening in protected enclaves. The goal is that the collective norms be observed and that only approved models and methods are employed. Enclaves are made to prevent anyone from seeing the data of another, including the model's central owner. The model's own intellectual property is also protected in a similar way [5].

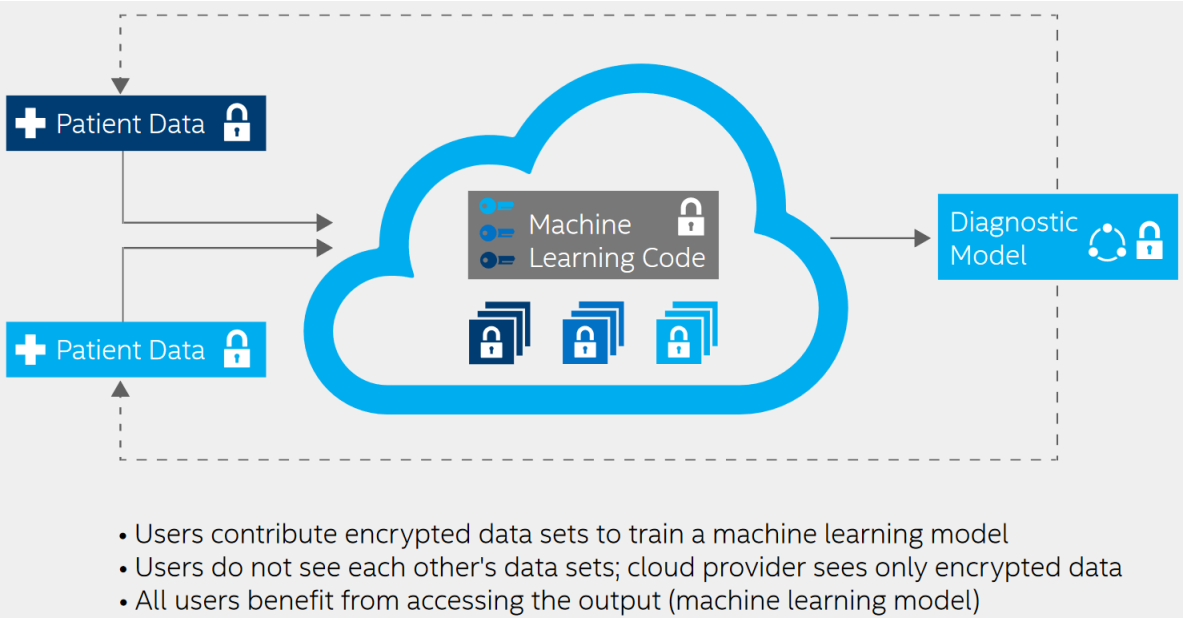

Figure 4.10: Use of CC in Healthcare, an example via Intel [5].

4.3.4 OpenMRS - Medical Record System

The Open MRS is an open-source record management system application based on Java language. Upon discussion, we chose to implement this application as a part of the Thesis Implementation. The Application is not developed using Confidential Computing methodologies. Please refer to Chapter 6 for the application demo.

4.4 EU Legal Requirements

The BDSG-new [77], or the New Federal Data Protection Act is so named because it took the place of the previous BDSG on May 25, 2018. It was updated in order to be at par with the GDPR and the EU-Privacy Directive for Policy and Justice (EU-Directive 2016/680). It makes sure that personal data is protected regardless of how it is processed—whether it is done using cutting-edge technology, like computer-based processing, or more conventional approaches. (Manual processing and paper records are examples of non-automated methods). In any case, the BDSG-new applies to any personal data intended to be a part of a file system. The day was significant because it brought into full force the new German Privacy Act (**Bundesdatenschutzgesetz**), often known as BDSG-new, and marked the beginning of

a new era in global data privacy with Europe's General Data Protection Regulation (GDPR). However, the GDPR supersedes the BDSG-new [78].

4.4.1 Gematik Rules - ePA

According to Gematik [79], Relevant data must always be accessible. The centerpiece of a digitally supported healthcare system is the electronic patient record or EPA. All pertinent health information about a patient or a patient is stored in the electronic patient record (EPA). For instance, medication details, doctor notes, or evidence are included. Suppose the person or a representative or a representative of the investment has yet to speak with someone about it. In that case, the health insurance companies (Krankenversicherungen) offer every insured patient (Versicherten) an ePA in which the data are protected and stored. Patients and patients have access to the data in their ePA in this situation. Individual medical facilities can be denied access to their data, or you can only transfer specific data sets.

All Patients currently only receive an ePA if they consciously want to do so ("Opt-in"). This will change in the future. The Health Ministry (Bundesgesundheitsministerium) will automatically create an ePA for every insured person in Germany as part of its digitization strategy, which was unveiled in March 2023. Whoever does not want an ePA must actively object ("Opt out"). The Ministry wants to see an "ePA for all" for about 80 percent of people by the year 2025.

New opportunities are provided by the ePA for all[79]:

- Accessible in a medical setting
- The secure location for health data
- Medicines management using the EPA
- Always available
- Using full Potential in the healthcare system
- Connected Health

The ePA [79] serves as the connecting link between clinical practice and research. In Germany, every person receives an ePA that allows them to provide data to their doctors and other healthcare providers. In contrast, doctors and nurses update the relevant ePA of their patients with the most recent findings, research findings, or other data.Pseudonymizable[1] ePA data of all patients are made available to the Research Data Center Health of the BfArM if the insured person uses their app and has not objected to the data being released. Researchers can identify patterns in disease, identify relationships between events, and create effective treatments using this data set. Then, these discoveries and techniques flow back into clinical practice, improving the entire healthcare system.

[1] Pseudonymization is a data management and de-identification process that substitutes one or more fictitious identifiers, or pseudonyms, for personally identifiable information fields inside a data record. The data record becomes less recognizable while still being appropriate for data analysis and data processing when a single pseudonym is used for each replaced field or group of replaced fields. A method of meeting the new General Data Protection Regulation (GDPR) requirements of the European Union for secure data storage of personal information is pseudonymization (or pseudonymization, the spelling according to European rules). When information that might be used to re-identify people is added, pseudonymized material can be returned to its original form. Anonymization, on the other hand, is meant to stop people from being re-identified inside the dataset.

ePA- Summary

To give individuals complete control over their health-related data, the electronic patient record (ePA) is being implemented in Germany. Consent is the legal justification for this processing. The use of the ePA is entirely up to the patient. What information is added to or removed from the ePA is decided by the patient. They control who has access to the ePA and have the power to completely remove it. Determine who has access to which document is saved in the ePA using your smart device, the insured person. Additionally, they have the option to make the data available for specific research projects. The Research Data Center, which serves as a trustee to make data available and an anonymization and pseudonymization center, makes this feasible. However, it is unclear from the law whether only German academic institutions may submit access requests to use the data for research purposes.

4.4.2 Literature Review - Legal Laws

Another informative article [80] summarizes that in Germany, the processing of health-related data by federal public authorities and processing by non-public organizations, such as privately held hospitals, is generally covered under the new Federal Data Protection Act (BDSG-new).

Laws in place for healthcare research

Only subsidiary public bodies of federal states are covered by the BDSG-new. When processing health-related data, hospitals must comply with state legislation, regardless of their ownership structures. In the case of publicly owned hospitals, state hospital regulations differ from state data protection legislation. Depending on the controller's nature and the entity's type (such as a public or private corporation), particular rules in the aforementioned legislation may apply to data processing for scientific research purposes. Recent Patient Data Protection Act regulations that concentrate on electronic patient files and set requirements in addition to the civil law provisions that apply to traditional patient files apply to healthcare data and its use for scientific research. All of the laws mentioned contain provisions relating to patients' rights, which must be applied in accordance with their relation lex specialis-lex generalis [2]. In the end, it is the responsibility of the competent federal and state supervisory bodies to supervise data protection. Data protection regulations must be administered concurrently with professional secrecy regulations. Professional norms and guidelines are crucial to compliance with research ethics, but institutional ethics committees will ultimately be in charge of conducting ethics audits.

Requirements for the legal processing of data for healthcare purposes

Health-related data may generally be processed in Germany for patient care in accordance with GDPR Art. 9(2)(h),(3) in combination with Art. 6(1)(b). The treatment contract serves as the legal foundation in this situation. Additionally, no provision of federal or state legislation precludes the explicit consent of the data subject from lifting the processing ban for sensitive data in Art. 9(1) GDPR, allowing for the direct application of Art. 9(2)(a). Sector-specific regulations for the processing of health-related data are based on Art. 9(4) GDPR, such as the requirement for written informed permission (§8 GDA) for genetic testing and analysis for medical purposes.

[2] A special law (lex specialis) takes precedence over a general law (lex generalis), according to the Lex specialis principle and thus has priority of application.

Requirements for using healthcare data for research purposes

This consent covers both the medical procedure and the processing of the associated data. Processing of patient data for the benefit of patient care is permitted by state hospital regulations, some of which expressly standardize consent-based processing. Although certain policies prioritize patients' consent, it is likely that the transfer of patient data from one service provider to another for the purpose of treatment will occur on the same legal basis as for the initial processing for the purpose of medical care. An additional data processing authorization for healthcare purposes is established by some federal state hospital statutes. According to the BDSG, professional secrecy laws must be applied independently and concurrently for data processing (1(2) BDSG). Numerous federal and state hospital legislation specify that processing of patient data is only permitted if it does not result in an unauthorized disclosure, as defined by Section 203 of the Criminal Code. Beyond regulations that expressly require the disclosure of personal information covered by professional secrecy, it is debatable whether additional data protection measures might qualify as a disclosure competence.

5 Design

Below are some of the prerequisites any realistic security architecture must meet to provide strongly protected software containers (like, for SGX/SEV). It is essential that we take this in mind while selecting the final Design of the system architecture. The final product however will be chosen by Semeco cluster in Dresden, Germany. But here are our suggestions:

1. Container Confidentiality - All data and code inside containers must be kept confidential at all times.
2. Container Integrity - Container integrity must be maintained both during use and while they are idle. Any attempts at altering should be either identified or stopped, to protect the freshness of data.
3. Protection against Malicious Host and VM - In the presence of a malicious host system, as well as malicious commodity and SEV VMs, confidentiality and integrity need to be ensured. Only then is a system faut-tolerant
4. Secure Communication - To allow secure container management, secure communication channels must be made available for the container and its provider.
5. Secure Deployment and Attestation - Each of the containers must be launched in the correct and expected state, and the status of each container must be attestation-verifiable remotely. It's better to have hardware attestation capabilities rather than relying only on the software.
6. Flexibility and Usability - To be widely adopted in practice, a solution must be quite usable and be integrated with the current software environment. There might be, however, a few changes required for the code, depending on the model of choice.
7. Off-the-shelf Hardware - Hardware changes shouldn't be needed to implement the solution. To be able to upgrade existing cloud servers, only off-the-shelf hardware components should be used. And, most importantly, the hardware has to be trusted at all times.
8. Low-Performance Overhead - To achieve a fair trade-off involving security and performance, the solution should have only a limited performance impact.

From what is seen and learned about Confidential Computing on the Cloud, it can be seen that one perfect solution doesn't exist, but multiple.

5.1 Solution 1: Microsoft Azure

From our preliminary research, it looks like Azure follows most of the design principles we established in the previous section. There are two ways of going with the deployment, as illustrated in the next two sections.

5.1.1 Ease of Use - Confidential VMs

This is the Virtual-machine-level confidentiality solution.

- Control - Works at the virtual machine level, allowing existing virtual machines to be migrated to take advantage of confidential memory operation.
- Security model - AMD SEV-SNP ensures the integrity and verifiability of virtual machine memory encryption.
- Effort - It is critical to transition virtualized workloads to a confidential computing environment as soon as possible.
- Use cases - Existing applications can benefit from a lift and shift deployment approach to confidential computing [81].

Under Azure, this approach is the easiest to implement as:

- Excellent for existing apps.
- Minimal effort required by everyone.
- PaaS solution.
- Hardware isolation is implemented - the CSP cannot access the Data/Code.
- However, Guest OS and Guest Admin are to be trusted.

5.1.2 More Control - Enclaves (SGX)

These are VMs with Application-level Enclaves [82].

- Control - Developers can benefit from line-by-line source code control for application workloads.
- Security model - Intel SGX enclaves are created by programs, and secure data is accessed from within the enclave.
- Effort - Allow enough time to plan and build a customized, secure virtual machine solution.
- Use cases - Customized software designed for confidential computing [81].

It is important to note about this solution that:

- Cannot be done for existing apps - too many changes to code required.
- Custom Apps can be made to suit both the CSP architecture and the customer.
- IaaS solution.
- Hardware isolation is implemented - the Guest Admin, the CSP, and the VM OS cannot access the Data/Code.

5.2 Solution 2: Open Telekom Cloud

The Bare Metal service offering on OTC is one where the developers can develop applications tailored to the customer. Here, existing applications can run smoothly without a problem, but it will be better to have confidential computing capabilities provided by Scontain as in the form of the product Scone. According to reports, future Attestation support is available through Intel's Project Amber - [70]. There has been work going on in this sector and more on this can be found in Chapter 4. Until this is released for the general public, we recommend using Scone for its attestation services using LAS and CAS and, for a worry-free implementation.

6 Implementation

6.1 Application Demo - OpenMRS

OpenMRS - Open Medical Record System [83] is a web-based electronic medical record that is Java-based. OpenMRS is a program as well as a community. It is a program that originally served as an electronic medical record system *EMR* for underdeveloped nations. It has developed into a medical informatics platform utilized on every continent thanks to its open-source community.

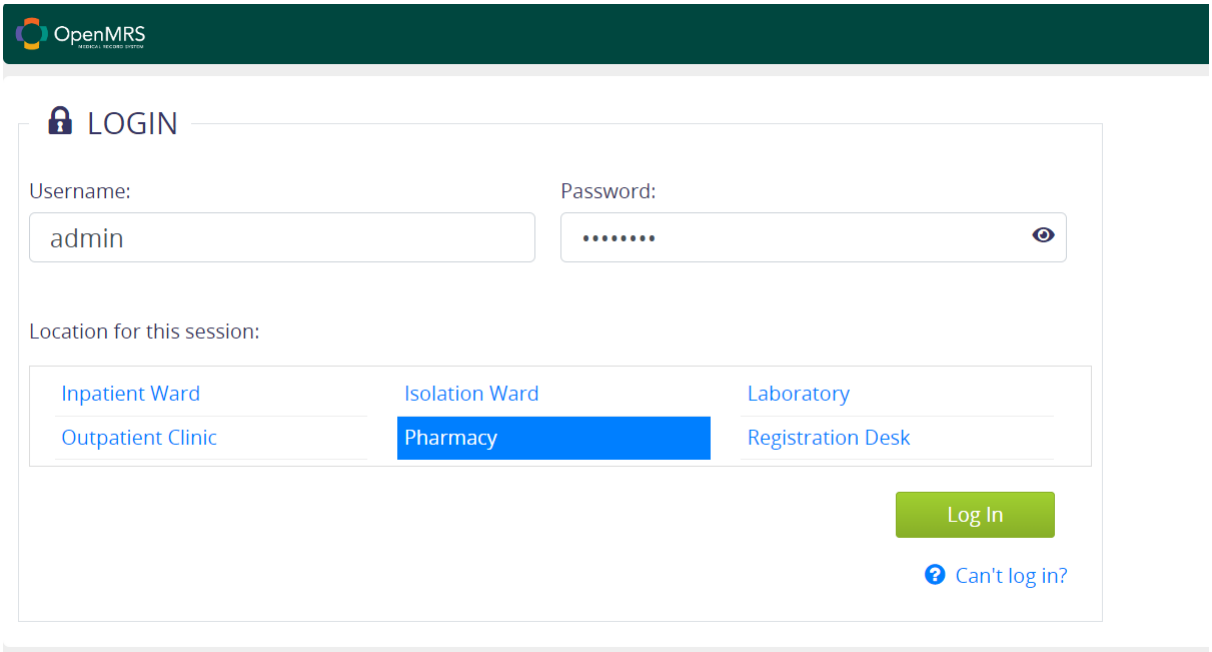

Figure 6.1: Demo: The OpenMRS login page where the doctors and authorized staff can enter the patient details and retrieve old records [84].

The login page shown in Fig. 6.1, separates you from functionality available to you at separate locations. So, if you log in with Pharmacy, you only see details relevant to you. This ensures the confidentiality of the information available to each user based on their role as a basic Identity and Access Management (IAM) protocol. OpenMRS began with a simple data model, wrapped it in an API, and then constructed a web-based application that makes use of the API. The OpenMRS API functions as a "black box," concealing the intricacies of the data model underlying it and ensuring that applications and modules that use the API adhere to

a consistent set of business rules for handling electronic medical record system data. It is built using three openmrs building blocks - Core Platform, Concept Dictionary, and Add-on Modules. A lot more can be learned from the video available on Youtube [85].

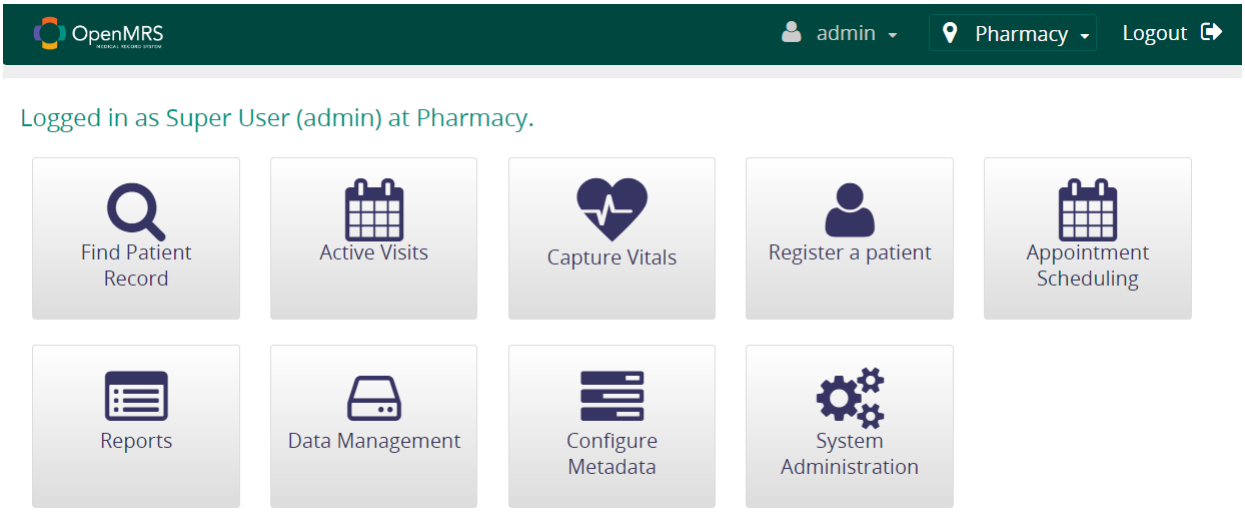

Figure 6.2: Demo: The OpenMRS Dashboard where all the function buttons are visible. The aim of the 2nd version of OpenMRS was to be able to provide an easy-to-use layout for doctors and nurses catering to patients in developing countries. [84].

OpenMRS is a system that defines unique ideas and observations using a concept dictionary. It was first constructed by converting paper forms to electronic forms and categorizing and arranging concepts into an electronic schema. This made data collection and usage in patient care more easier. Data is increasingly being input directly via web-based forms or mobile applications. Modules are supported by OpenMRS, allowing implementations to change the system's behavior without requiring agreement.

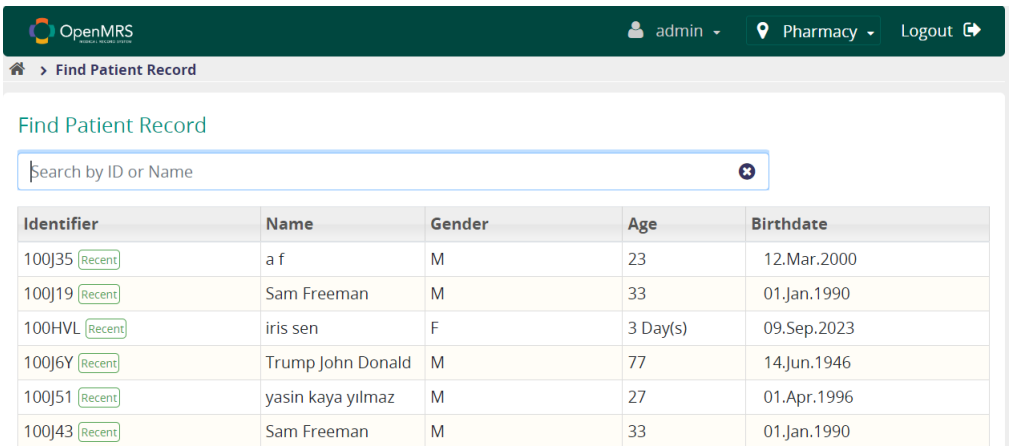

Figure 6.3: Demo: The OpenMRS Records page with sample patient records [84].

Modules have complete system access, which allows them to add tables, change API behavior, and edit web pages. Individuals, companies, government aid groups, non-governmental organizations, and for-profit and charitable enterprises all contribute to OpenMRS. The entire program is open source and is available online [83].

With the application demo available [84], the screenshots demonstrate how one can operate the application after setting it up, as shown in Fig. 6.1, Fig. 6.2, Fig. 6.3, and Fig. 6.4.

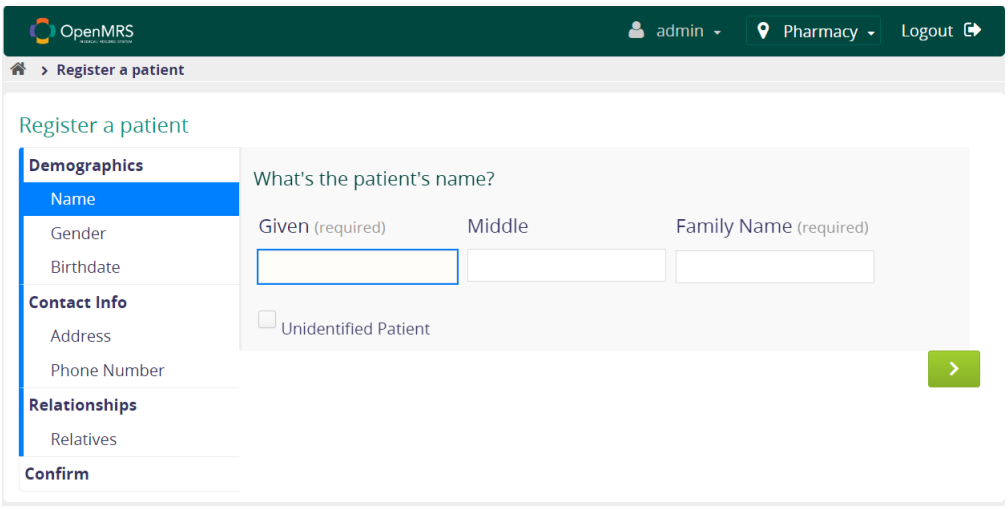

Figure 6.4: Demo: The OpenMRS Register Patient page where the doctors can enter essential details and register the patient with the respective hospital or clinic [84].

6.2 Microsoft Azure

As per the initial research, it would be better to deploy the application on a CVM if it has Intel SGX compatibility. However, from what is known from the tutorial present at the Microsoft website [86], the machines listed - DC(number)sv2, DC(number)sv3, and DC(number)dsv3 - are not available in Germany region, and only in Europe region as of the time of writing this Thesis report [87]. For processing e-health data of German citizens in compliance with the legal laws around data protection, it is important that the data stays in and is processed in EU, preferably Germany. The special Azure regions have some service offerings in Germany (a special region) but not the kind of VMs we require for this thesis [88].

From the installation steps present on the Developer's page of the OpenMRS application [89], we pick the one where it's installed using docker-compose. It is using docker that we initialize an application without worrying much about the environment. This is done via containers.

Azure - Confidential Virtual Machine (CVM)

The following steps were taken to achieve the successful setup:

1. Login to the Azure portal with your ID and Password. For this, we used the credentials provided to us by our company. Upon successful login, go ahead and create a VM. Choose an appropriate Subscription and Resource group.

2. Name the virtual machine - in our case - mnkh-thesis. Select the region - in our case - West Europe, Security Type - Confidential Virtual Machines, Image: Ubuntu Server 20.04 LTS Confidential VM x64 Gen2, and Size: **Standard DC2ads v5** - 2 vcpus, 8 GiB memory. The current cost for the machine mentioned is €64.90 per month. Dadsv5-Type1 in the Azure domain is a dedicated Host SKU that uses the AMD EPYC 7763v processor. It can be scaled up to 64 physical cores, 112 vCPUs, and 768 GiB of RAM.

3. Authentication Type - Password. Choose Username and Password. All other settings can be left to default under the sections Disks, Networking, Management, Monitoring, Advanced, and Tags. Click on 'Review + Create'. Wait for the VM to be deployed. After that Login into the machine using the console.

4. Install mysql, docker, and docker-compose in the newly setup VM using the guides available at [90, 91, 92]. Remember to follow the steps carefully and complete the Post-installation steps in case of Docker installation on Linux. The password chosen during the installation of MySQL must be noted down carefully. In case the default is missing, the root user password should be 'password'.

5. Using the steps available on [89] set up the OpenMRS on the VM using the provided docker-compose.yml file provided under the Option 3 heading.

6. Run the software using the command 'docker-compose up -d'.

7. Errors we face: Port 3306 busy -> Kill the port 3306 using - sudo kill 'sudo lsof -t -i:3306'.

8. To further use the software, we have to use a remote desktop connection to the Azure VM. A helpful guide from Microsoft is available [93].

As highlighted above, the DCadsv5 series are confidential virtual machines for use in confidential Computing [94]. These private virtual machines are powered by AMD's third-generation EPYCTM 7763v CPU in a multi-threaded configuration having up to 256 MB L3 cache. These CPUs have a maximum frequency boost of 3.5 GHz. **Secure Encrypted Virtualization Secure Nested Paging (SEV-SNP)** is available in both series. SEV-SNP provides hardware-isolated virtual machines (VMs) that safeguard data from other virtual machines, the hypervisor, and the host administration code. Confidential virtual machines provide hardware-based VM memory encryption. These series additionally provide OS disk pre-encryption prior to VM deployment using various key management techniques.

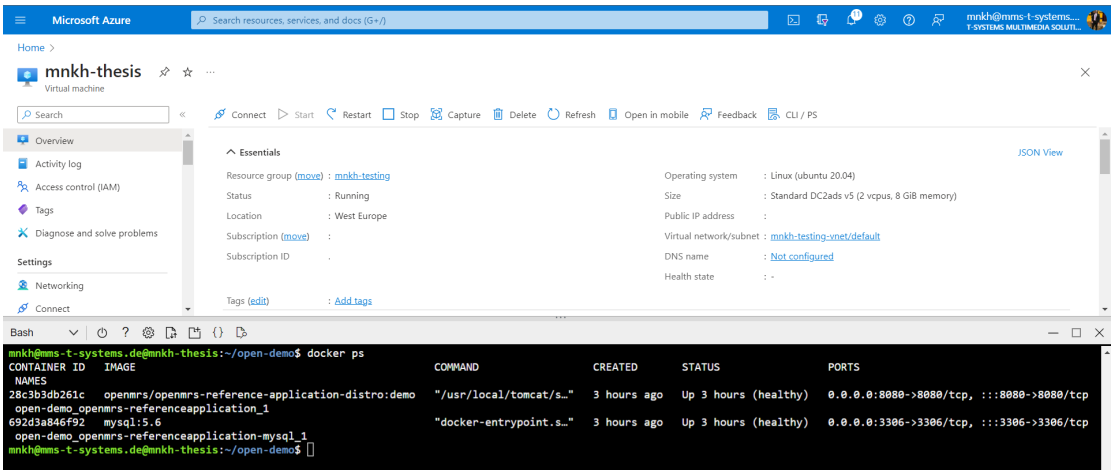

Figure 6.5: The Screenshot of successful implementation of the OpenMRS e-health records.

Azure - VMs with application enclaves

The following steps were taken to achieve the successful setup:

1. Login to the Azure portal with your ID and Password. For this, we used the credentials provided to us by our company. Upon successful login, go ahead and create a VM. Choose an appropriate Subscription and Resource group.

2. Name the virtual machine - in our case - mnkh-thesis-enclave. Select the region - in our case - West Europe, Security Type - Trusted Launch, Image: Ubuntu Server 20.04 LTS Confidential VM x64 Gen2, and Size: **Standard DC2s v3** - 2 vcpus, 16 GiB memory. The current cost for the machine mentioned is €119.43 per month.

3. Authentication Type - Password. Choose Username and Password. All other settings can be left to default under the sections Disks, Networking, Management, Monitoring, Advanced, and Tags. Click on 'Review + Create'. Wait for the VM to be deployed. After that Login into the machine using the console.

4. Install mysql, docker, and docker-compose in the newly setup VM using the guides available at [90, 91, 92]. Remember to follow the steps carefully and complete the Post-installation steps in case of Docker installation on Linux. The password chosen during the installation of MySQL must be noted down carefully. In case the default is missing, the root user password should be 'password'.

5. Using the steps available on [89] set up the OpenMRS on the VM using the provided docker-compose.yml file provided under the Option 3 heading.

6. Run the software using the command 'docker-compose up -d'.

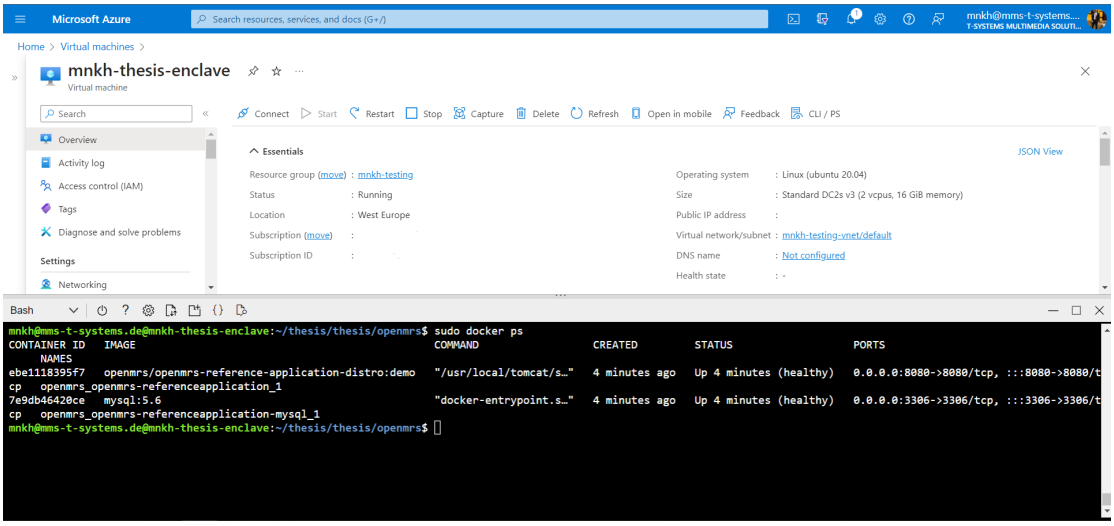

Figure 6.6: The Screenshot of successful implementation of the OpenMRS e-health records on Azure VM.

These were the 2 ways to include CC support in Azure. The implementations are quite similar and the basic differences lie in the basic architecture. The first one, machine DC2adsv5 provides Virtual-machine-level confidentiality and machine DC2sv3 provides VMs with application enclaves. The latter provides the developer with more control over the functioning of the VM and here, the developers can develop secure enclave-based applications to run in these VMs to protect application data and code in use. The former provides a lift-and-shift approach for existing workloads and protects data from the cloud operator with VM-level confidentiality. And, another important distinction would be that the DC2adsv5 machine has AMD SEV as the TEE while the DC2sv3 machine has Intel SGX. From our comparison of TEEs in Chapter 2, it is better to go with Intel SGX.

6.3 Open Telekom Cloud (OTC)

In a similar way, from the installation steps present at the Developer's page of the OpenMRS application [89], we pick the one where it's installed using docker-compose. The following steps were taken to achieve the successful setup:

1. Login into the Open Telekom Cloud (OTC) homepage. Click on Bare Metal Server offering and then Allocate BMS. Select the following options. Region: eu-de, AZ: eu-de-02, BMS Name: mnkh-thesis, Flavor: **physical.i7n.28xlarge.4**, Image: Standard Ubuntu 22.04 amd64 uefi BMS latest, VPC: vpc-default, Security Group: default, NIC: subnet-default(192.168.0.0/24), EIP: No EIP bound to the primary network interface, Key Pair: KeyPair-ef21, and Quantity: 1. the cost of the setup is exorbitantly high at 6.80 €/hour. The Key Pair here is generated at the time of allocation of the BMS and can be later on used to remotely access the machine via SSH.

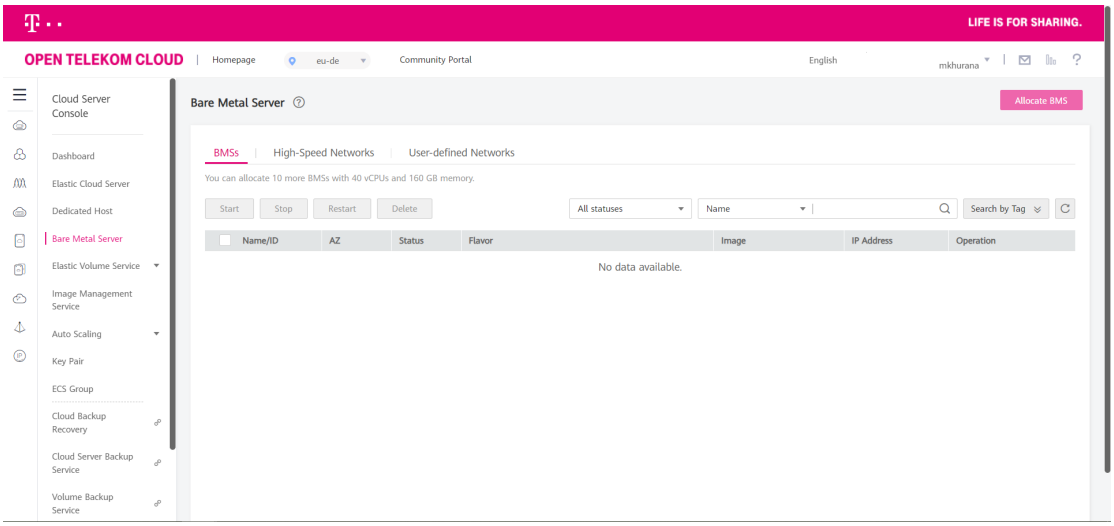

Figure 6.7: The Open Telekom Cloud (OTC) dashboard after login.

2. The machine can then be connected to using the WSL2 Ubuntu distribution or via Putty, on Windows- using SSH. Proceed with the implementation in a similar manner to the one done above, in Azure CVM implementation.

3. Since this offering is a Bare-metal hardware solution over the cloud, we also need to set up the Linux OS before proceeding with the next few steps. It is important we check the image compatibility with the underlying TEE of our choice before we start the setup. For our convenience, the bare metal server came preconfigured with Ubuntu 22.04 image, making it easier for us to connect with the machine.

4. Install mysql, docker, and docker-compose in the newly setup VM using the guides available at [90, 91, 92]. Remember to follow the steps carefully and complete the Post-installation steps in case of Docker installation on Linux. The password chosen during the installation of MySQL must be noted down carefully. In case the default is missing, the root user password should be 'password'.

5. Using the steps available on [89] set up the OpenMRS on the VM using the provided docker-compose.yml file provided under the Option 3 heading.

6. Run the software using the command 'docker-compose up -d'. After the Application is up and running, as shown by the docker ps command on the terminal in Fig. 6.9, one can visit http://localhost:8080/openmrs/ to see the dashboard. However, we might have to run 'service mysql status/stop' depending on the usage of port 3306. If it is busy, then the application container might not start up.

7. The Bare Metal server offering is SGX enabled, as learned before in Chapter 3.

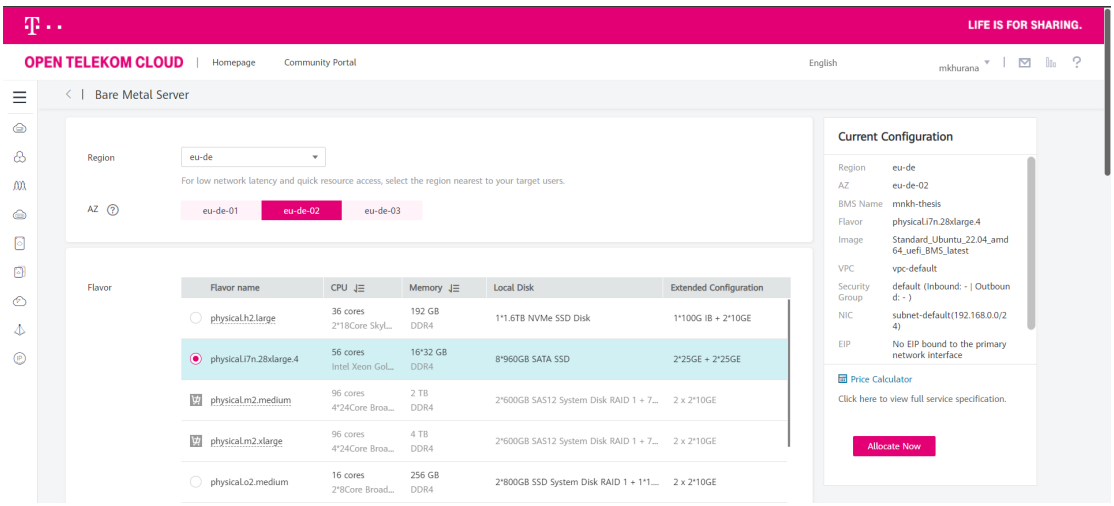

Figure 6.8: The specifications of the confidential Bare Metal Server (BMS) allocated for the application.

```
ubuntu@mnkh-thesis:~/thesis/thesis/openmrs$ docker ps
CONTAINER ID   IMAGE                                                COMMAND                  CREATED          STATUS                    PORTS
          NAMES
29a78b28c981   openmrs/openmrs-reference-application-distro:demo    "/usr/local/tomcat/s…"   7 minutes ago    Up 7 minutes (healthy)    0.0.0.0:8080->8080/tcp, :::8080->8
080/tcp   openmrs_openmrs-referenceapplication_1
7def4e001254   mysql:5.6                                            "docker-entrypoint.s…"   52 minutes ago   Up 7 minutes (healthy)    0.0.0.0:3306->3306/tcp, :::3306->3
306/tcp   openmrs_openmrs-referenceapplication-mysql_1
ubuntu@mnkh-thesis:~/thesis/thesis/openmrs$
```

Figure 6.9: The Open Telekom Cloud (OTC) hosting the OpenMRS application.

It is important to note here that more functionalities can be added here via the addition of the SCONE framework. As learned before in Chapter 4, scone provides us with Attestation capabilities that are essential for a Confidential computing environment. The configuration and installation of Scone is getting better each day and we hope to add it in the future iteration of the final product, if OTC is selected as the choice of platform by the SEMECO cluster for their computing needs. This will provide us with a lot more managed services and more scalable solutions at the end.

7 Evaluation

This thesis project aims to provide a solution to the data leaks affecting the healthcare industry. The solution provided here is implemented using Confidential Computing technology. The aim of the Confidential paradigm is to protect the data while it is in use. There are already encryption methods available to protect data at rest and data in transit. For the thesis, we wanted to provide a choice of solutions that can be chosen by Semeco cluster in Dresden, Germany.

For the implementation part, we chose an open-source light-weight application that handles e-health data records of patients in a hospital. The application is easy to use and is designed for hospital physicians and staff members, focusing mainly on developing countries.

The implementation of the existing application OpenMRS was first tried on the native system. The machine used is an IBM Thinkpad with an Intel(R) Core(TM) i7-8665U CPU @ 1.90GHz with 32 GiB of RAM and 512 GiB of storage running a Windows 10 Enterprise Edition OS. The experience of implementing it was easy and quick. We experimented here with various ways of installing the OpenMRS software and the docker-compose file method seemed the easiest. Hence, this was the preferred method of implementation in the Azure VMs and on OTC BMS machines. For the most part, it can be understood that the application does not need a lot of processing power to run smoothly. It comes down to how big the data is, on which the search and retrieval is happening in MySQL.

In Azure, we tried two different Confidential Cloud offerings. The application OpenMRS was deployed and, it ran successfully on both machines as seen in Chapter 6. The basic difference between these two was that Machine 1 has an AMD SEV-enabled processor (AMD EPYCTM 7763v CPU) and Machine 2 has an Intel SGX enabled (3rd Gen Intel Xeon Scalable processor). The SGX-enabled machine is costly and it provides us with VMs with application enclaves as the AMD SEV machine provides us with a Confidential VM. They are both secure, scalable, robust, and fault-tolerant. However, for its Attestation capability, as of the time of writing this report, we need to rely on the Azure Attestation service. The role of Attestation is to provide a report as to which hardware exactly is the machine running on. Azure does this efficiently but with it's own parameters. We are not saying that it is false, but it has to be trusted as that is the only way the Attestation can happen. The report received shows Azure machine parameters which are derived versions of the actual received parameters. So the need to trust Azure, the provider, with the Attestation might not be the best idea. We need our data secured from the Cloud Service Provider.

For Open Telekom Cloud, we allocated a Bare Metal Server along with a fresh copy of the Ubuntu 22.04 image. On this OS, we implemented our application. It was deployed and it ran successfully as observed in Chapter 6. For Attestation and other services, we can deploy

the SCONE solution by Scontain. It will enhance the security as we will have to trust the CSP only for the infrastructure and hence vendor exclusion will be observed. The cost of the BMS setup is extremely high, and then to add on the cost of scone functionalities, it will be quite secure but a costly option.

Attribute	Microsoft Azure	Open Telekom Cloud
Offers	Azure provides two levels of Confidential VMs - VM level confidentiality and VMs with application enclaves.	OTC provides for a Bare Metal Server.
Machine specifications	AMD SEV-enabled processor (AMD EPYCTM 7763v CPU) and Intel SGX-enabled (Intel Xeon Scalable processors).	Intel SGX-enabled (Intel Xeon Gold 6348).
GDPR Compliance (Legal)	GDPR Compliant. Although, machines in Region West Europe, and not Germany.	GDPR Compliant. Machines available in Germany.
Attacker model	Fulfils attacker model except for trust on - Attestation service. Operator Exclusion possible. CSP cannot access data.	Fulfils attacker model, as it is Bare Metal Machine with Ubuntu image. Operator Exclusion possible.
Cost	AMD Machine - 65€/month, Intel machine - 119.43€/month.	Costly - 6.80€/hour.
Attestation	Provided by Azure Attestation Service.	No support yet. Available soon. Until then - SCONE services (recommended).
Developer Experience	Easy to follow, connect and implement. Connection with SSH and auto-shutdown capabilties tested.	Takes a lot of time to boot-up and hard to follow guides.SSH connection possible.

Table 7.1: Differences in implementation of Azure and Open Telekom Cloud.

8 Conclusion

We learned how costly an affair it is for a data breach in the healthcare industry. It is the one industry with the highest losses in the event of a data loss or data leak. Data leak in itself is a serious issue and when it comes to e-health data, it is a crucial life-and-death scenario. There, just cannot be a leak. As this might contain the most personal, confidential details of the citizens of the country. Leakage of which could lead to some dangerous macro-economic consequences. Data resides in three states, at rest, in transit, or when it is being used/processed. Most technologies of today provide protection for the data at rest and for data in transit. This is where Confidential Computing methodology comes in for rescue. With various functionalities like Hardware Attestation, it aims to protect data when it is being processed. A lot of previous literature was researched and upon careful discussion, the choice of elements (TEEs, frameworks, CSPs) was made and the solution was designed. This was done keeping in mind the attacker model, the trust assumptions, and the Legal requirements of Data processing in Germany (EU - GDPR). A final and complete cloud stack with Confidential computing can be materialized in multiple ways. The proposed solutions for the Semeco cluster were implemented on Microsoft Azure and on Open Telekom Cloud. The differences and similarities in these solutions were documented and presented.

Bibliography

[1] *Cost of a data breach 2022 | IBM*. https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700074839479712&p5=p&gclid=Cj0KCQiA6LyfBhC3ARIsAG4gkF-UqmjCJIUf8Dq-y2QYt_QHEyQdGIJJ-1eqoNvGfW-JBKP4zep12iYaAgaDEALw_wcB&gclsrc=aw.ds. (Accessed on 04/04/2023).

[2] *Confidential computing for next-generation cybersecurity - Edgeless Systems*. https://www.edgeless.systems/confidential-computing/. (Accessed on 09/01/2023).

[3] *CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf*. https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf. (Accessed on 04/11/2023).

[4] *Azure Confidential Computing Overview | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/confidential-computing/overview. (Accessed on 05/22/2023).

[5] Intel. *An introduction to Confidential Computing - Solution brief*. https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/intro-to-confidential-computing-solution-brief.pdf. (Accessed on 05/28/2023).

[6] Keke Chen. "Confidential High-Performance Computing in the Public Cloud". en. In: arXiv:2212.02378 (Dec. 2022). arXiv:2212.02378 [cs]. URL: http://arxiv.org/abs/2212.02378.

[7] *Common Terminology for Confidential Computing - PDF*. https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/Common-Terminology-for-Confidential-Computing.pdf. (Accessed on 04/11/2023).

[8] Pulse and Arm. *confidential-computing-pulse-survey.pdf*. https://armkeil.blob.core.windows.net/developer/Files/pdf/graphics-and-multimedia/confidential-computing-pulse-survey.pdf. (Accessed on 05/20/2023). Feb. 2021.

[9] Jia Zhiguang. *When Kubernetes Encounters Confidential Computing, How Does Alibaba Protect the Data in the Container? - Alibaba Cloud Community*. https://www.alibabacloud.com/blog/when-kubernetes-encounters-confidential-computing-how-does-alibaba-protect-the-data-in-the-container_597363. (Accessed on 05/23/2023). Feb. 2021.

[10] Ashish Kumar. *Top Confidential Computing Companies - MarkTechPost*. https://www.marktechpost.com/2022/09/01/top-confidential-computing-companies/. (Accessed on 06/22/2023). Sept. 2022.

[11] *Confidential Computing 101 by Felix Schuster (Edgeless Systems) | OC3 2021 - YouTube*. https://www.youtube.com/watch?v=77U12Ss38Zc&t=847s. (Accessed on 04/09/2023).

[12] Muhammad Usama Sardar and Christof Fetzer. "Confidential computing and related technologies: a critical review". en. In: *Cybersecurity* 6.1 (May 2023), p. 10. ISSN: 2523-3246. DOI: 10.1186/s42400-023-00144-1.

[13] Liang Zhou. *Remote Attestation EAA: The Final Link for Secure Deployment of Confidential Containers - Alibaba Cloud Community*. https://www.alibabacloud.com/blog/599074. (Accessed on 09/01/2023). June 2022.

[14] Muhammad Usama Sardar. "Understanding Trust Assumptions for Attestation in Confidential Computing". en. In: *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*. Baltimore, MD, USA: IEEE, June 2022, pp. 49–50. ISBN: 978-1-66540-260-6. DOI: 10.1109/DSN-S54099.2022.00028. URL: https://ieeexplore.ieee.org/document/9833797/.

[15] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. "The role of the adversary model in applied security research". en. In: *Computers and Security* 81 (Mar. 2019), pp. 156–181. ISSN: 01674048. DOI: 10.1016/j.cose.2018.12.002.

[16] Ophélie Surcouf. *Confidential Computing: A History*. https://blog.mithrilsecurity.io/title-confidential-computing-a-history-ft-apple-intel-and-the-linux-foundation/. (Accessed on 09/11/2023). Aug. 2023.

[17] Victor Costan and Srinivas Devadas. *Intel SGX Explained*. Cryptology ePrint Archive, Paper 2016/086. https://eprint.iacr.org/2016/086. 2016. URL: https://eprint.iacr.org/2016/086.

[18] *Intel Software Guard Extensions SGX | Bare Metal Servers | OVHcloud*. https://www.ovhcloud.com/en/bare-metal/intel-software-guard-extensions/. (Accessed on 04/11/2023).

[19] *What is Intel SGX (Software Guard Extensions)?* https://www.trentonsystems.com/blog/what-is-intel-sgx. (Accessed on 04/11/2023).

[20] Chia-Che Tsai, Donald E Porter, and Mona Vij. "Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX". en. In: ().

[21] Saeid Mofrad et al. "A comparison study of intel SGX and AMD memory encryption technology". en. In: *Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy*. Los Angeles California: ACM, June 2018, pp. 1–8. ISBN: 978-1-4503-6500-0. DOI: 10.1145/3214292.3214301. URL: https://dl.acm.org/doi/10.1145/3214292.3214301.

[22] Tu Dinh Ngoc. "Everything You Should Know About Intel SGX Performance on Virtualized Systems". en. In: 3.1 ().

[23] Pau-Chen Cheng et al. "Intel TDX Demystified: A Top-Down Approach". en. In: arXiv:2303.15540 (Mar. 2023). arXiv:2303.15540 [cs]. URL: http://arxiv.org/abs/2303.15540.

[24] *Where Is a List of Processors that Support Intel® Software Guard...* https://www.intel.com/content/www/us/en/support/articles/000028173/processors.html. (Accessed on 09/01/2023).

[25] David Kaplan, Jeremy Powell, and Tom Woller. "AMD memory encryption". In: *White paper* (2016).

[26] Ralph Palutke, Andreas Neubaum, and Johannes Götzfried. "SEVGuard: Protecting User Mode Applications Using Secure Encrypted Virtualization". en. In: *Security and Privacy in Communication Networks*. Ed. by Songqing Chen et al. Vol. 305. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Cham: Springer International Publishing, 2019, pp. 224–242. ISBN: 978-3-030-37230-9. DOI: 10.1007/978-3-030-37231-6_12. URL: http://link.springer.com/10.1007/978-3-030-37231-6_12.

[27] Ferdinand Brasser et al. "Trusted Container Extensions for Container-based Confidential Computing". en. In: arXiv:2205.05747 (May 2022). arXiv:2205.05747 [cs]. URL: http://arxiv.org/abs/2205.05747.

[28] J. Alex Halderman et al. "Lest we remember: cold-boot attacks on encryption keys". en. In: *Communications of the ACM* 52.5 (May 2009), pp. 91–98. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/1506409.1506429.

[29] Jeremy Powell. *AMD SEV-SNP Attestation: Establishing Trust in Guests*. https://www.amd.com/content/dam/amd/en/documents/developer/lss-snp-attestation.pdf. (Accessed in May 2023). Sept. 2022.

[30] Scott Thornton. *Arm TrustZone explained*. https://www.microcontrollertips.com/embedded-security-brief-arm-trustzone-explained/. (Accessed on 05/26/2023). Dec. 2017.

[31] Xupeng Li et al. "Design and Verification of the Arm Confidential Compute Architecture". en. In: ().

[32] *Introduction to DevOps on AWS - AWS Whitepaper*. https://docs.aws.amazon.com/pdfs/whitepapers/latest/introduction-devops-aws/introduction-devops-aws.pdf. (Accessed on 05/03/2023). Apr. 2023.

[33] David Brown. *Confidential computing: an AWS perspective | AWS Security Blog*. https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/. (Accessed on 05/03/2023). Aug. 2021.

[34] Matt Koop. *Bare metal performance with the AWS Nitro System | AWS HPC Blog*. https://aws.amazon.com/blogs/hpc/bare-metal-performance-with-the-aws-nitro-system/. (Accessed on 05/03/2023). Aug. 2021.

[35] *PDF: What is AWS Nitro Enclaves? - AWS*. https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html. (Accessed on 09/01/2023).

[36] *PDF: Using cryptographic attestation with AWS KMS - AWS*. https://docs.aws.amazon.com/enclaves/latest/user/kms.html. (Accessed on 09/14/2023).

[37] *PDF: Enabling multi party analysis of sensitive data using AWS Nitro Enclaves*. https://d1.awsstatic.com/events/Summits/reinvent2022/CMP403_Enabling-multi-party-analysis-of-sensitive-data-using-AWS-Nitro-Enclaves-.pdf. (Accessed on 09/01/2023).

[38] *Google Cloud Platform: A cheat sheet | TechRepublic*. https://www.techrepublic.com/article/google-cloud-platform-the-smart-persons-guide/. (Accessed on 04/11/2023).

[39] *Security, Privacy, and Cloud Compliance | Google Cloud*. https://cloud.google.com/security. (Accessed on 04/11/2023).

[40] *Confidential Computing concepts | Confidential VM | Google Cloud*. https://cloud.google.com/compute/confidential-vm/docs/about-cvm. (Accessed on 04/23/2023).

[41] *Build an isolated Private Network for your Servers - vRack| OVHcloud*. https://www.ovhcloud.com/en-gb/network/vrack/. (Accessed on 06/05/2023).

[42] *What is confidential computing? | OVHcloud*. https://www.ovhcloud.com/en/bare-metal/uc-confidential-computing/. (Accessed on 05/27/2023).

[43] OVHcloud and Securitee. *Maximum flexibility and scalability as a reliable basis for Confidential Computing - Case Study*. https://www.ovhcloud.com/sites/default/files/casestudy/case-study_securitee_ovhcloud_en_032022.pdf. (Accessed on 05/27/2023). Mar. 2022.

[44] Alibaba Cloud. *How Alibaba Protects the Data in the Container: Confidential Computing, Inclavare Containers and ACK-TEE | Medium*. https://alibaba-cloud.medium.com/when-kubernetes-encounters-confidential-computing-how-does-alibaba-protect-the-data-in-the-a2d19e8619dd. (Accessed on 05/28/2023). Apr. 2022.

[45] Vikas Bhatia. *Navigating confidential computing across Azure*. https://techcommunity.microsoft.com/t5/azure-confidential-computing/navigating-confidential-computing-across-azure/ba-p/2520752. (Accessed on 05/22/2023). July 2021.

[46] *Azure confidential computing products | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/confidential-computing/overview-azure-products. (Accessed on 05/22/2023). Dec. 2022.

[47] Microsoft Research. *What is CCF? - CCF documentation*. https://microsoft.github.io/CCF/main/overview/what_is_ccf.html. (Accessed on 05/22/2023).

[48] *Enclave aware containers on Azure | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/confidential-computing/enclave-aware-containers. (Accessed on 05/22/2023).

[49] Raki Rahman. *Secure a web app architecture with Azure confidential computing*. https://techcommunity.microsoft.com/t5/azure-confidential-computing/secure-a-web-app-architecture-with-azure-confidential-computing/ba-p/2598108. (Accessed on 05/22/2023). Oct. 2021.

[50] Thomas Van Laere. *Thomas Van Laere | Azure Confidential Computing: IaaS*. https://thomasvanlaere.com/posts/2022/04/azure-confidential-computing-iaas/. (Accessed on 05/22/2023). Apr. 2022.

[51] Thomas Van Laere. *Azure Confidential Computing: Confidential VMs*. https://thomasvanlaere.com/posts/2022/06/azure-confidential-computing-confidential-vms/. (Accessed on 05/22/2023). June 2022.

[52] Michael McReynolds. *Preview: Introducing DCesv5 and ECesv5-series Confidential VMs with Intel TDX - Microsoft Community Hub*. https://techcommunity.microsoft.com/t5/azure-confidential-computing/preview-introducing-dcesv5-and-ecesv5-series-confidential-vms/ba-p/3800718. (Accessed on 07/03/2023). Apr. 2023.

[53] *Evolving Zero Trust - How real-world deployments and attacks are shaping the future of Zero Trust strategies*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT. (Accessed on 06/05/2023). Nov. 2021.

[54] *microsoft/CCF: Confidential Consortium Framework*. https://github.com/Microsoft/CCF. (Accessed on 05/22/2023).

[55] *Open Telekom Cloud | European Alternatives*. https://european-alternatives.eu/product/open-telekom-cloud. (Accessed on 05/28/2023).

[56] *Confidential Computing - Open Telekom Cloud*. https://open-telekom-cloud.com/de/sicherheit/confidential-computing. (Accessed on 05/28/2023).

[57] Open Telekom Cloud. *Bare Metal Server: Dedizierter Cloud Server - Open Telekom Cloud*. https://open-telekom-cloud.com/de/produkte-services/core-services/bare-metal-server. (Accessed on 05/28/2023).

[58] Carmelo Pino and Roberto Di Salvo. "A Survey of Cloud Computing Architecture and Applications in Health". In: *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*. Atlantis Press, 2013, pp. 1649–1653. ISBN: 978-90-78677-61-1. DOI: 10.2991/iccsee.2013.413. URL: https://doi.org/10.2991/iccsee.2013.413.

[59] Mohemmed Sha M and Mohamudha Parveen Rahamathulla. "Cloud-based Healthcare data management Framework". In: *KSII Transactions on Internet and Information Systems (TIIS)* 14.3 (2020), pp. 1014–1025.

[60] Fernaz Narin Nur and Nazmun Nessa Moon. "Health care system based on cloud computing". In: *Asian Transactions on Computers* 2.5 (2012), pp. 9–11.

[61] Lena Griebel et al. "A scoping review of cloud computing in healthcare". In: *BMC medical informatics and decision making* 15.1 (2015), pp. 1–16.

[62] Fangjian Gao, Scott Thiebes, and Ali Sunyaev. "Rethinking the Meaning of Cloud Computing for Health Care: A Taxonomic Perspective and Future Research Directions". In: *J Med Internet Res* 20.7 (Sept. 2018), e10041. ISSN: 1438-8871. DOI: 10.2196/10041. URL: http://www.ncbi.nlm.nih.gov/pubmed/29997108.

[63] Lingkiswaran Devadass, Sugalia Santhira Sekaran, and Rajermani Thinakaran. "Cloud computing in healthcare". In: *International Journal of Students' Research in Technology & Management* 5.1 (2017), pp. 25–31.

[64] Maulik Parekh and B Saleena. "Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis". In: *Procedia Computer Science* 50 (2015), pp. 537–542.

[65] Mu-Hsing Kuo et al. "Opportunities and challenges of cloud computing to improve health care services". In: *Journal of medical Internet research* 13.3 (2011), e1867.

[66] Lidong Wang and Cheryl Alexander. "Medical Applications and Healthcare Based on Cloud Computing". In: *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* 2 (Oct. 2013). DOI: 10.11591/closer.v2i4.3452.

[67] Sungyoung Oh et al. "Architecture design of healthcare software-as-a-service platform for cloud-based clinical decision support service". In: *Healthcare informatics research* 21.2 (2015), pp. 102–110.

[68] Chen Changming. "Research on the Application of Cloud Computing in Medical Field". In: *Big Data and Cloud Innovation* 1.1 (2017).

[69] Stephen Jepsen. *Store, Protect, Optimize Your Healthcare Data with AWS: Part 2 | AWS Architecture Blog*. https://aws.amazon.com/blogs/architecture/store-protect-optimize-your-healthcare-data-with-aws-part-2/. (Accessed on 04/11/2023). Oct. 2018.

[70] *Project Amber*. https://projectamber.intel.com/. (Accessed on 07/31/2023). Mar. 2022.

[71] Sergei Arnautov et al. "SCONE: Secure Linux Containers with Intel SGX". en. In: (Nov. 2016).

[72] *Fortanix Runtime Encryption® Platform - Whitepaper*. https://resources.fortanix.com/rteplatform-whitepaper/. (Accessed on 07/30/2023). 2019.

[73] Amar Gowda. *Healthcare platform confidential computing - Azure Example Scenarios | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/architecture/example-scenario/confidential/healthcare-inference. (Accessed on 05/22/2023).

[74] *Confidential computing application enclave nodes on Azure Kubernetes Service (AKS) | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-nodes-aks-overview. (Accessed on 05/22/2023).

[75] E-PIX - Record Linkage. *E-PIX Record Linkage und Identitätsmanagement*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ths-greifswald.de/wp-content/uploads/2022/12/e-pix_Broschuere_V06_Stand_1-Dez.pdf. (Accessed on 05/29/2023).

[76] *E-PIX® – Independent Trusted Third Party*. https://www.ths-greifswald.de/en/researchers-general-public/e-pix/. (Accessed on 04/24/2023).

[77] Christoph. *Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) German Law Archive*. https://germanlawarchive.iuscomp.org/?p=712. (Accessed on 05/23/2023). Aug. 2017.

[78] Peter Oladimeji. *Germany's data privacy protection laws: Everything you need to know | Didomi*. https://shorturl.at/rMOV8. (Accessed on 05/23/2023). Mar. 2023.

[79] *Gematik ePA fuer alle PDF (SECURED, Deutsch)*. https://www.gematik.de/media/gematik/Medien/ePA/Dokumente/gematik_ePA_fuer_alle_print.pdf. (Accessed on 05/23/2023). Apr. 2023.

[80] Fruzsina Molnár-Gábor et al. "Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden". en. In: *Seminars in Cancer Biology* 84 (Sept. 2022), pp. 271–283. ISSN: 1044579X. DOI: 10.1016/j.semcancer.2021.12.001.

[81] *When to use application enclaves versus VM-level confidentiality - Training | Microsoft Learn*. https://learn.microsoft.com/en-us/training/modules/intro-to-confidential-computing-with-azure-virtual-machines/when-to-use-application-enclaves. (Accessed on 09/01/2023).

[82] *Build with SGX enclaves - Azure Virtual Machines | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-computing-enclaves. (Accessed on 09/09/2023).

[83] *Introduction to OpenMRS - Documentation - OpenMRS Wiki*. https://wiki.openmrs.org/display/docs/Introduction+to+OpenMRS. (Accessed on 09/01/2023).

[84] *Demo – OpenMRS.org*. https://openmrs.org/demo/. (Accessed on 09/01/2023).

[85] *Global Goods: OpenMRS - YouTube*. https://www.youtube.com/watch?v=h0Z-_SSZaCY&t=11s&ab_channel=TechChange. (Accessed on 09/01/2023).

[86] *Quickstart - Create Intel SGX VM in the Azure Portal | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/confidential-computing/quick-create-portal. (Accessed on 09/01/2023).

[87] *Azure Products by Region | Microsoft Azure*. https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/?products=virtual-machines&regions=non-regional,germany-north,germany-west-central. (Accessed on 09/01/2023).

[88] *Azure regions - Azure Virtual Machines | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/virtual-machines/regions. (Accessed on 09/10/2023).

[89] *Installing OpenMRS on Docker - Documentation - OpenMRS Wiki*. https://wiki.openmrs.org/display/docs/Installing+OpenMRS+on+Docker. (Accessed on 09/01/2023).

[90] *How To Install MySQL on Ubuntu 20.04 | DigitalOcean*. https://www.digitalocean.com/community/tutorials/how-to-install-mysql-on-ubuntu-20-04. (Accessed on 09/01/2023).

[91] *Install Docker Engine on Ubuntu | Docker Docs*. https://docs.docker.com/engine/install/ubuntu/. (Accessed on 09/01/2023).

[92] *How To Install and Use Docker Compose on Ubuntu 20.04 | DigitalOcean*. https://www.digitalocean.com/community/tutorials/how-to-install-and-use-docker-compose-on-ubuntu-20-04. (Accessed on 09/01/2023).

[93] *Connect using Remote Desktop to an Azure VM running Windows - Azure Virtual Machines | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/virtual-machines/windows/connect-rdp. (Accessed on 09/01/2023).

[94] *Azure DCasv5 and DCadsv5-series confidential virtual machines - Azure Virtual Machines | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/virtual-machines/dcasv5-dcadsv5-series. (Accessed on 09/01/2023).