Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS
Analisi e prevenzione

5 maggio 2025 (riveduta)

Valutazione tecnologica

Confidential computing

1 Introduzione

La sicurezza dei processi per l'elaborazione delle informazioni nei sistemi IT rappresenta un grande problema, in particolare alla luce del crescente uso del «cloud computing» e dei relativi servizi. Mentre il salvataggio e la trasmissione di dati possono essere garantiti agevolmente tramite procedura crittografica, l'elaborazione sicura dei dati[1] costituisce ancora oggi una delle sfide cruciali: come elaborare dati in modo sicuro se non si è in grado di controllare fattivamente il software (code) preposto alla loro elaborazione e l'ambiente di esecuzione messo a disposizione dal provider del cloud? In passato sono stati sviluppati diversi approcci per trovare possibili soluzioni, che in parte sono stati anche attuati.

Nel quadro della presente valutazione tecnologica viene presentato brevemente uno di questi approcci risolutivi, ovvero il «confidential computing», approfondendo soprattutto di cosa si tratta, come funziona fondamentalmente, quali sono i vantaggi e gli svantaggi, quali offerte concrete esistono sul mercato e come valutare le prospettive future.

2 Presentazione della problematica

Come accennato nell'introduzione, un'elaborazione sicura dei dati in un sistema IT costituisce una grande sfida: infatti è necessario garantire sia l'integrità dell'ambiente in cui l'applicazione viene eseguita (cioè l'ambiente di esecuzione) sia la confidenzialità dei dati durante l'elaborazione. Come mostrato nella figura 1, l'ambiente di esecuzione non comprende solo l'applicazione stessa (inclusi dati e code) che viene eseguita in una macchina virtuale (MV), bensì anche il sistema operativo ospite della MV nonché l'hypervisor, il sistema operativo host e l'hardware.[2] Tutte queste componenti devono essere protette da una compromissione e da un'esfiltrazione di dati per scongiurare che la sicurezza dell'applicazione possa venire

[1] In questo contesto si parla ad esempio anche di «data in use» (in contrapposizione a «data at rest», per i dati salvati, e a «data in transit» per i dati trasmessi).

[2] Se si rinuncia a utilizzare una MV e, quindi, anche a una virtualizzazione quanto più ampia possibile, allora la situazione di partenza si semplifica e l'applicazione può essere eseguita direttamente nell'hardware e nel sistema operativo host.

intaccata. Nella figura 1 le componenti in colore rosso sono critiche per la sicurezza dell'elaborazione dei dati e vanno accettate come affidabili[3].

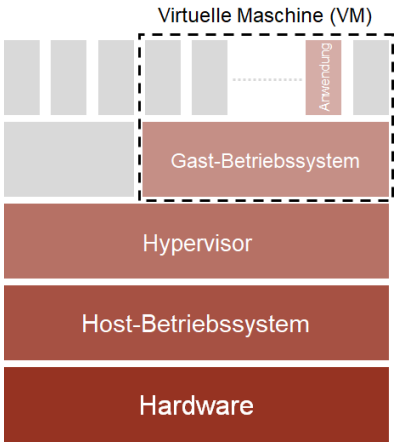

Figura 1: elaborazione dei dati in un sistema IT

Se un'applicazione non viene eseguita a livello locale («on premises»), affidandosi piuttosto ai servizi di un provider di cloud, allora la persona che effettua l'elaborazione dei dati deve potere contare non solo sull'affidabilità dei propri sistemi IT, ma anche sull'affidabilità del provider e dei suoi sistemi IT. Questa situazione è raffigurata schematicamente nella figura 2. La persona che effettua l'elaborazione dati invia i dati e il code al provider del cloud, che applica il code ai dati in un ambiente di esecuzione da lui stesso messo a disposizione e, al termine, fornisce il risultato (in maniera sicura e garantita) alla persona che effettua l'elaborazione dei dati. Da notare che di regola la persona che effettua l'elaborazione dei dati non ha alcuna possibilità di controllare direttamente l'ambiente di esecuzione e la sua sicurezza: in altre parole essa deve potersi fidare di quanto promesso dal provider del cloud nonché dei relativi certificati e attestazioni.

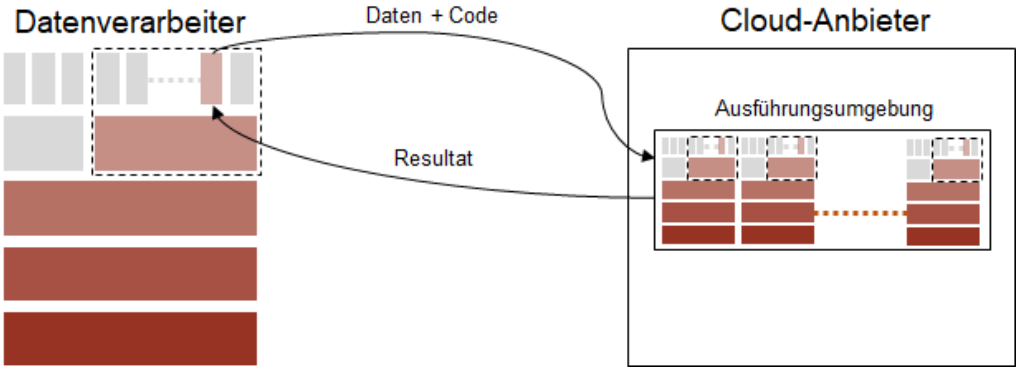

Figura 2: l'esecuzione di un'applicazione nel quadro del «cloud computing»

La problematica insita in questa situazione è descritta in letteratura, ad esempio anche in relazione alla «secure remote computation»: come si può mettere a disposizione un ambiente

[3] Nella sicurezza IT le componenti (di sistema) la cui sicurezza non può venire né dimostrata né verificata vanno accettate come affidabili. Esse costituiscono nel loro insieme la «trusted computing base» (TCB) che deve essere mantenuta quanto più ridotta possibile.

di esecuzione affidabile in un'infrastruttura IT gestita da terzi e non controllabile direttamente e come impedire efficacemente l'esfiltrazione di dati, in modo tale che nel complesso ne risulti un'elaborazione «sicura» dei dati? Tale quesito ribalta la problematica della protezione di un'infrastruttura IT affidabile da un code potenzialmente malevolo (ad. esempio gli applet Java), che può venire risolta almeno in parte con il sandboxing. Nel caso del sandboxing l'ambiente di esecuzione è tenuto ai minimi termini e separato dal resto dell'infrastruttura IT (ovvero isolato) per impedire che un codice potenzialmente malevolo possa influenzare l'ambiente stesso o comprometterlo. Il sandboxing non è un'opzione per la «secure remote computation» poiché appunto non è l'infrastruttura IT a dovere venire protetta, bensì i dati e il code. Per il problema legato alla «secure remote computation» occorrono altri approcci risolutivi, che di solito sono più complessi.

3 Approcci risolutivi

A lungo termine la soluzione del problema legato alla «secure remote computation» sarà sicuramente trovata grazie a procedure di cifratura integralmente omomorfe. Con questo tipo di procedure la persona che effettua l'elaborazione dati può mettere a disposizione i suoi dati al provider del cloud in forma cifrata cosicché quest'ultimo possa sì elaborarli ma non riesca a decifrarli: vi è così la garanzia che il provider del cloud non possa vedere i dati in chiaro. Al termine dell'elaborazione dei dati, il risultato viene riconsegnato sempre in forma cifrata alla persona che effettua l'elaborazione dei dati, che ora può decifrare il risultato. In tal modo è possibile approntare una soluzione realizzabile via software al problema legato alla «secure remote computation». Purtroppo però le procedure di cifratura integralmente omomorfe ad oggi note e disponibili sono ancora troppo poco efficienti per potere essere utilizzate in compiti generici di elaborazione dati.

Nell'attesa che siano disponibili procedure di cifratura integralmente omomorfe adatte alla pratica si può cercare di risolvere il problema legato alla «secure remote computation» con l'aiuto di componenti hardware affidabili, garantendo così in una certa qual misura l'integrità dell'ambiente di esecuzione. Esistono componenti hardware affidabili di vario tipo, come ad esempio le smartcard, gli elementi di sicurezza, i moduli hardware di sicurezza e i «trusted platform modules» (TPMs). Quest'ultimi sono specificati nel quadro dell'iniziativa «Trusted Computing» del «Trusted Computing Group» (TCG[4]) e sono stati impiegati su larga scala. Ad esempio nei sistemi IT comunemente in commercio è possibile garantire con l'aiuto di un TPM che il sistema venga fatto partire in uno stato definito («bootet») e, quindi, che non sia stato compromesso da un software manipolato. Così si può assicurare l'integrità dell'ambiente di esecuzione, almeno fino al momento in cui un software sconosciuto non venga caricato ed eseguito nel sistema. Visto però che prima o poi ciò accadrà, l'onere generato dall'utilizzo di un TPM è comunque relativamente elevato rispetto ai benefici.

Una possibilità più semplice e più ampiamente utilizzabile per il supporto hardware è stata proposta da un consorzio industriale[5] ed è stata denominata «confidential computing»: l'hardware fornisce la possibilità di gestire un cosiddetto «trusted execution environment» (TEE) come «enclave sicura» in cui l'elaborazione dati può svolgersi in modalità garantita e sicura: in concreto, l'elaborazione avviene unicamente nel processore e nessun software al di fuori dell'applicazione che gestisce il TEE può accedere al TEE né leggere dati da quest'ultimo. Inoltre l'applicazione prima di caricare i dati può convalidare sia il TEE sia il code che va eseguito nel TEE (si parla di «remote attestation»). Affinché le variabili di stato e i risultati

[4] https://trustedcomputinggroup.org

[5] https://confidentialcomputing.io

possano comunque venire salvati provvisoriamente, il TEE supporta un cosiddetto «sealing», cioè una protezione crittografica dei dati in una memoria di archiviazione prevista a tale scopo. Le chiavi che sono necessarie per la «remote attestation» e il «sealing» esistono unicamente nell'hardware o nei relativi TEE e non possono venirvi letti, o solo con un onere sproporzionatamente elevato.

L'esecuzione di un'applicazione ricorrendo a un TEE è mostrata nella figura 3. Da notare che, in questo scenario, le uniche componenti affidabili sono l'applicazione medesima e il TEE (entrambi sono evidenziati in colore rosso nella figura). In particolare il gestore di un sistema IT non può visionare i dati dell'applicazione, perlomeno fintantoché l'hardware usa correttamente le caratteristiche necessarie al «confidential computing». In concreto questo significa che è necessario fidarsi del fornitore dell'hardware.

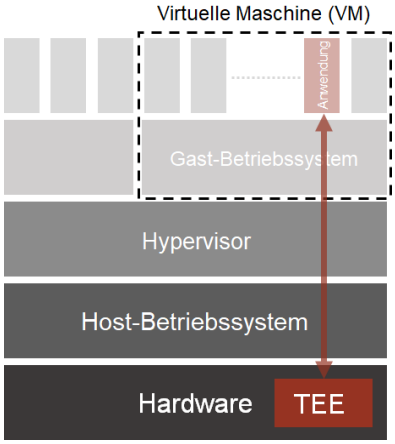

Figura 3: esecuzione di un'applicazione ricorrendo a un TEE

L'impiego del «confidential computing» in un ambiente cloud si profila come molto interessante e promettente. La situazione dell'illustrazione 2, ampliata così da comprendere anche il «confidential computing», è raffigurata schematicamente nell'illustrazione 4. I dati e il code vengono immessi nel TEE del provider del cloud da parte della persona che effettua l'elaborazione dati: così sono codificati «end-to-end» e vengono decodificati soltanto nel TEE. Poiché sono eseguiti solo nel TEE, il provider del cloud (quale gestore dell'ambiente di esecuzione, rispettivamente del TEE) non ha alcuna possibilità di visionare i dati o il code e, quindi, di compromettere l'elaborazione dei dati. Il TEE mette quindi a disposizione un ambiente di esecuzione sicuro e garantito, la cui integrità è tale da potere convalidare l'applicazione stessa. Con l'aiuto della «remote attestation» è possibile assicurare che sia il TEE sia il code in esso eseguito siano autentici e che l'elaborazione dati si svolga correttamente, a tutto vantaggio della persona che effettua l'elaborazione dati. Il risultato viene messo a disposizione dell'applicazione direttamente da parte del TEE che consente l'elaborazione dati. Ovviamente la sicurezza dell'elaborazione dati dal lato del cliente (rispettivamente, nella figura 4, della persona che effettua l'elaborazione dati) continua a essere dipendente da tutte le componenti. Invece, dal lato del provider del cloud, le interdipendenze e l'affidabilità necessaria possono venire fortemente ridotte. Di conseguenza anche il provider del cloud può sottrarsi alla responsabilità poiché fondamentalmente non ha alcuna possibilità di visionare i dati o di compromettere il code.

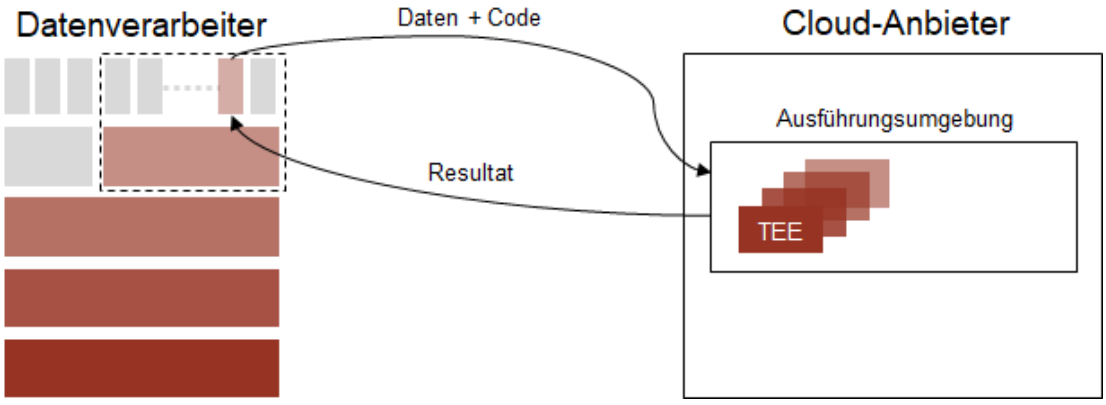

Figura 4: esecuzione di un'applicazione ricorrendo a un TEE in un ambiente cloud

4 Panoramica del mercato

Il termine «confidential computing» designa l'approccio tecnologico o risolutivo appena illustrato che viene attuato e implementato in modi diversi dai vari produttori di processori. Per principio esistono due approcci:

- da un lato, un produttore può attuare e implementare il «confidential computing» in modo tale che singole applicazioni o loro parti rilevanti per la sicurezza (ad esempio in un container) vengano esercitate in un TEE, mentre altre applicazioni e parti siano eseguite al di fuori del TEE. Gli esempi più noti di tale approccio sono il software «Guard Extensions (SGX)» di Intel [1] e «TrustZone» di ARM;
- d'altro lato, un produttore può anche attuare e implementare il «confidential computing» in modo tale che intere MV (con tutte le applicazioni ivi eseguite) siano esercitate in un TEE. Gli esempi più famosi sono «TDX» di Intel [2],« Secure Encrypted Virtualization (SEV[6])» di AMD e l'attuazione del «confidential computing» nei processori specializzati di NVIDIA.[7]

Entrambi gli approcci comportano vantaggi e svantaggi. Mentre il primo approccio può venire esercitato in maniera selettiva (ovvero vanno eseguite in un TEE solo le applicazioni critiche o parti di esse), invece il secondo approccio è del tipo «in blocco» poiché intere MV vengono eseguite in un TEE. Nell'impiego pratico il secondo approccio risulta più semplice: infatti non è necessario determinare le applicazioni in vista del fatto che vengano esercitate in un TEE, ma basta unicamente spostarle.

Sulla base dei processori oggigiorno disponibili che attuano in vario modo il «confidential computing» esistono anche hyperscaler emergenti a livello internazionale che offrono diversi servizi nell'ambito del «confidential computing». Le seguenti informazioni vanno intese unicamente a titolo di esempio perché, ben inteso, vi sono anche altri hyperscaler e provider di cloud che propongono servizi simili (come ad esempio Alibaba con «Enclave VM»). La situazione di mercato in questo ambito è molto dinamica, ma è anche di difficile comprensione a causa delle diverse terminologie utilizzate.

[6] Come descritto in https://www.amd.com/en/developer/sev.html, la «SEV» esiste in diverse versioni, come ad esempio «SEV-ES (SEV Encrypted State)» e «SEV-SNP (SEV Secure Nested Paging)».

[7] https://www.nvidia.com/en-us/data-center/solutions/confidential-computing/

- Microsoft è già molto avanti in questo ambito e nel suo cloud «Azure» offre molti servizi di «confidential computing» orientati agli specifici vantaggi e svantaggi dei diversi processori.[8] In particolare propone anche un apposito servizio in relazione all'«Azure Kubernetes Service (AKS)».
- Google persegue parimenti una strategia diversificata a livello di servizi, anche se il fulcro della sua offerta è costituito dalle «confidential VMs». Analogamente a Microsoft con «AKS», Google nel quadro del suo «Google Kubernetes Engine (GKE)» propone anche «Confidential GKE Nodes» e supporta il «confidential computing» per applicazioni IA/AA altamente performanti sui processori specializzati di NVIDIA sopracitati.
- Amazon Web Services (AWS) sulla base del proprio sistema «Nitro» – da essa stessa sviluppato e che viene utilizzato per la virtualizzazione e il funzionamento automatizzato di istanze «Elastic Compute Cloud (EC2)» – ha ideato le «Nitro Enclaves» che consentono di attuare enclavi sicure nell'ottica del «confidential computing». In un'enclave «Nitro» è possibile incapsulare ed esercitare parti critiche per la sicurezza di un'istanza «EC2» (come ad esempio un sistema per la gestione delle chiavi).

Inoltre nell'ambito del «confidential computing» vi è anche un folto e crescente numero di fornitori specializzati di prestazioni di servizi in grado di offrire aiuto in caso di domande e progetti concreti, come ad esempio «Decentriq»[9] e CYSEC[10] in Svizzera o «enclaive»[11] in Germania.

5 Potenziale e prospettive future

Con l'aiuto del «confidential computing» e dei TEE corrispondenti è possibile impostare l'elaborazione dati in maniera più sicura e, nel contesto del «cloud computing», in modo anche meno dipendente dall'affidabilità del o dei provider di cloud. L'approccio per risolvere il problema della «secure remote computation» è quindi interessante e fornisce un contributo importante al miglioramento della sovranità digitale in un mondo sempre più orientato al «cloud computing». È lecito prevedere che (oltre a Intel SDX e TDX, ARM TrustZone, AMD SEV e NVIDIA) sul mercato arriveranno anche altre implementazioni che saranno impiegate nei centri di calcolo degli hyperscaler e in altri provider di cloud. Ciò vale però soprattutto per le offerte cloud nel senso di «Infrastructure-as-a-Service (IaaS)» e di «Platform-as-aService (PaaS)», mentre in misura minore per il «Software-as-a-Service (SaaS)». Se le offerte vengono utilizzate in modo sensato è possibile garantire e rendere sicure in particolare anche le applicazioni con cui i dati vanno protetti nei confronti dei provider di cloud, come ad esempio la gestione di chiavi crittografiche o il confronto di dati rilevanti ai fini della protezione dei dati (un esempio di spicco è costituito dal confronto dei dati personali di contatto nel «messenger signal end-to- end» di cifratura).

Nonostante i suoi vantaggi, il «confidential computing» non è però la panacea destinata a risolvere tutti i problemi della sicurezza IT (nel caso di IaaS e PaaS). Anche se esso consente di ridurre la dipendenza dall'affidabilità dei provider di cloud, tuttavia sorge una nuova dipendenza: l'affidabilità dei TEE deve essere garantita e resa sicura. Un provider di cloud potrebbe infatti collaborare con un fornitore allo scopo di compromettere congiuntamente

[8] Una panoramica a questo proposito è disponibile ad esempio su https://learn.microsoft.com/en-us/azure/confidential-computing/overview-azure-products.

[9] https://www.decentriq.com

[10] https://www.cysec.com

[11] https://www.enclaive.io

un'elaborazione dati in un TEE. Però una simile collaborazione è sicuramente difficile da realizzare nella pratica ed è ancora più arduo mantenerla segreta. In definitiva possono venire attaccate anche implementazioni di «confidential computing» e i relativi TEE: gli attacchi più rilevanti (soprattutto temporizzati) sfruttano canali laterali.[12] Benché molti di questi attacchi siano puramente teorici ed evidenzino «soltanto» le possibilità potenziali, tuttavia inizierà un «gioco del gatto e del topo» tipico per la sicurezza IT: in altre parole, anche in futuro sarà necessario studiare gli attacchi conosciuti analizzandone requisiti e condizioni quadro per potere stimare in maniera precisa le ripercussioni sulle soluzioni e sulle offerte cloud realmente esistenti. Inoltre va sottolineato che spesso, nell'ambito della sicurezza IT, simili stime sono complesse da effettuare e richiedono assolutamente un'elevata competenza specialistica. Comunque dal punto di vista della tecnica di sicurezza, niente impedisce di impiegare il «confidential computing» e i relativi TEE: queste soluzioni e offerte andrebbero anzi utilizzate per applicazioni tecniche di sicurezza nella misura più ampia possibile, sempre se ciò è economicamente giustificabile.

Abbreviazioni

GKE	Google Kubernetes Engine
IaaS	Infrastructure-as-a-Service
IT	Tecnologia dell'informazione (acronimo in inglese: «Information Technology IT»)
IA	Intelligenza artificiale
AA	Apprendimento automatico
PaaS	Platform-as-a-Service
SaaS	Software-as-a-Service
SEV	Secure Encrypted Virtualization
SEV-ES	SEV Encrypted State
SEV-SNP	SEV Secure Nested Paging
SGX	Software Guard Extensions
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
VM	Macchina virtuale

Bibliografia

[1] V. Costan und S. Devadas, *Intel SGX Explained*, IACR Cryptology ePrint Archive, vol. 2016, n. 086, https://eprint.iacr.org/2016/086.pdf

[2] Intel, *Intel Trust Domain Extensions*, White Paper, attualizzato a febbraio 2023

[3] A. Muñoz, R. Ríos, R. Román und J. López, *A Survey on the (In)security of Trusted Execution Environments*, Computers & Security, vol. 129, giugno 2023, 103180, https://www.sciencedirect.com/science/article/pii/S0167404823000901

[4] A. Nilsson, P. Nikbakht Bideh und J. Brorsson, *A Survey of Published Attacks on Intel SGX*, arXiv: 2006.13598, attualizzato a giugno 2020, https://arxiv.org/abs/2006.13598

[12] In [3] sono riportati molti attacchi conosciuti contro diversi TEE (e in [4] sono riportati esclusivamente attacchi contro «Intel SGX»).