Solution Brief

Intel Security

Technology for Justice

Confidential Computing and the Fight to End Modern Slavery

A Human Rights Tragedy of the 21st Century

In today's modern world, most people see slavery as a historical phenomenon. While the media occasionally covers stories about victims, we tend to think of slavery and human trafficking as tragedies whose time has passed.

Not so. Most people today would be shocked to know that there are more than 50 million human beings trapped in slavery today, more than at any point in history.[1] Slavery in the 21st century is a crime that takes many forms, including sexual exploitation (primarily of women and children), forced labor, domestic servitude, criminal exploitation, organ harvesting, and forced marriage. It also includes human trafficking and smuggling, which often involves recruiting individuals through threats, force, fraud, coercion, or deception on the part of criminals in positions of power.

Standing in opposition to these crimes are groups such as **Hope for Justice**, a non-governmental organization working to end modern slavery and human trafficking and protect the rights of victims and survivors. Founded in 2008, Hope for Justice works to prevent human trafficking; to investigate and identify cases and accompany survivors as they claim their rights to justice, protection, and redress; and to partner with survivors' and other civil society organizations, companies, and governments to address the root causes of people's vulnerability to modern slavery.

Data as a Tool for Justice

In combating modern slavery, data plays a role that is hard to overstate. Imitating legitimate businesses, criminal organizations that profit from human exploitation are skilled at using data and technology to advance their efforts. In response, institutions and organizations like Hope for Justice are looking to harness technology and data to close the technology gap, utilizing it as a tool for good.

Globally, organizations working on cases of human trafficking have collected large pools of valuable data on both victims of slavery and perpetrators, as well as contextual information relating to emerging patterns and trends.

Victim data is incredibly sensitive and invariably includes personally identifiable information, while data on perpetrators may include the financial flows and organizational structures of criminal enterprises. All of this data is crucial information towards effective investigation and mitigation. However, if this sensitive data is leaked via mismanagement, rogue actors, or cyber threats, it can result in dire consequences for victims, compromise investigations, and hinder prosecutions. As a result, the safest approach for each organization has been to keep all information private, with little or no data exposed to any other actor. However, these relatively strict data practices can also slow or hinder effective investigations and interventions, especially where there are concerns for the safety of an individual. To date, anti-trafficking forces have lacked the tools to overcome the fears around data privacy and securely share data to extract information crucial to the fight for human dignity.

Confidential Computing

Intel and R3 enabled Hope for Justice to take advantage of Confidential Computing—a technology that enables sensitive data to be processed confidentially, out of view from unauthorized software or system administrators.

Confidential Computing enables encrypted data to be processed in memory while lowering the risk of exposing it to the rest of the system, thereby reducing the likelihood that sensitive data will be compromised. In addition, it provides a higher degree of control and transparency for users in multi-tenant environments where data can be isolated from other privileged portions of the system stack.

With its focus on securing data and code during processing, Confidential Computing relies on hardware-based controls such as the Trusted Execution Environments (TEEs) enabled by Intel® Software Guard Extensions (Intel® SGX) enclaves. Intel SGX helps provide protection for applications and data independent of the operating system or hardware configuration. This enables multiple organizations to collaborate on shared analyses and validate algorithms while shielding their confidential information or regulated data from the other parties. Intel SGX:

- Helps protect against software attacks, even when other elements of the stack are compromised.
- Helps increase protection for secret content (personally identifiable information and data, sensitive legal information, keys, etc.).
- Provides options for hardware-based attestation to validate code and signatures.

Confidential Computing lies at the heart of the Intel-R3-Hope for Justice collaboration.

The Intel-R3-Hope for Justice Project

The goal of the joint project between Intel, R3, and Hope for Justice is to build the Private Data Exchange (PDEx), a powerful application to be offered to the global movement to end human trafficking. PDEx enables the various organizations working against slavery to confidentially pool data related to individual cases. After data from these groups is uploaded, the application aggregates and analyzes it, then notifies appropriate agencies when relevant data matches are uncovered.

Given the sensitivity of the data, maintaining high security and compliance is mission-critical. To reap the benefits of collaboration, each organization must trust its data will be kept confidential and private, and the integrity of that data will be ensured. R3's Conclave platform is specifically designed to deliver this high level of protection. By leveraging the built-in security and attestation features of Intel SGX, Conclave provides organizations with increased confidence that information about the victims of slavery or those seeking to help them won't be exposed.

The Hope for Justice application workflow:

1. Case data from participating organizations is manually uploaded.
2. The data is encrypted and passed to Conclave instances shared by the various organizations.
3. The application scans the data to ensure it is appropriately formatted. This takes place within an Intel SGX enclave.
4. The matching code runs inside an Intel SGX enclave so all records are encrypted and inaccessible from outside.
5. Alerts are sent to the appropriate agencies, notifying them that a relevant match has been discovered.

Application Workflow

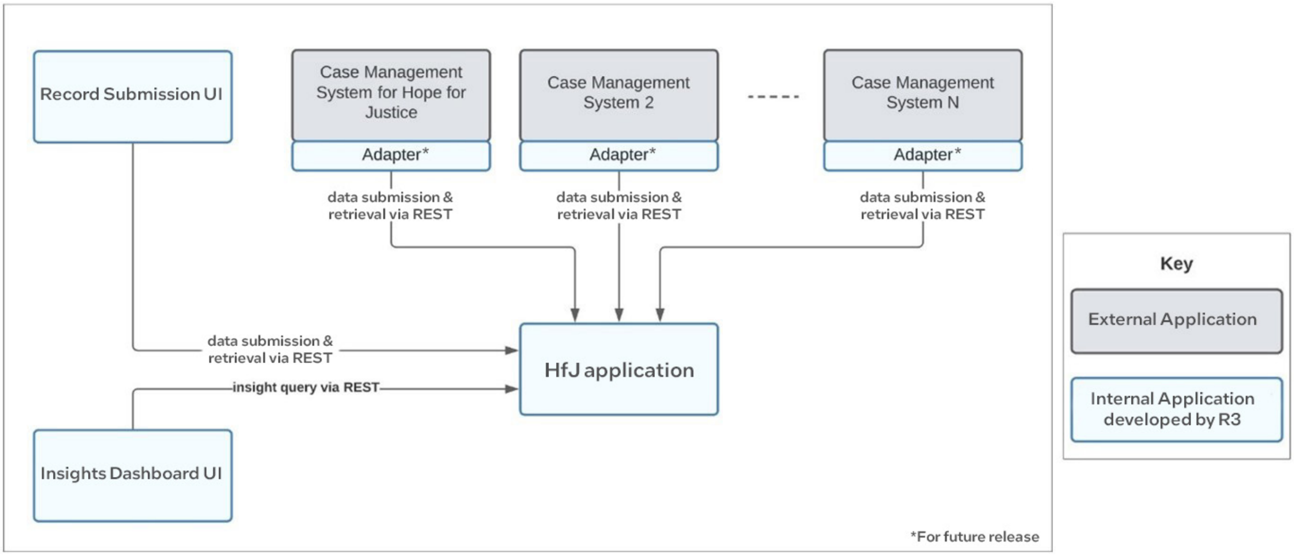
Record Submission UI
Case Management System for Hope for Justice
Adapter*
Case Management System 2
Adapter*
Case Management System N
Adapter*
data submission & retrieval via REST
data submission & retrieval via REST
data submission & retrieval via REST
data submission & retrieval via REST
insight query via REST
HfJ application
Insights Dashboard UI
Key
External Application
Internal Application developed by R3
*For future release

Figure 1: Systems context of the Hope for Justice Private Data Exchange application

Real-world Consequences

The match information will enable participating organizations to realize tangible outcomes in the fight against slavery. For instance:

- Perpetrator matching. If the same person appears in multiple matches, they may be involved in numerous cases of trafficking and be a serial offender or part of organized crime. The appropriate group can begin an investigation or notify law enforcement.
- Victim family name matching. Discovering the same surname in multiple cases may indicate that two or more family members have been trafficked separately. Linking the two cases may accelerate rescue and help reunite the family.
- Address matching. If the same property keeps showing up in results, it may be owned or operated by perpetrators or criminal organizations. This can be enough to trigger an investigation.
- Less obvious matches may not result in immediate investigations but can reveal previously unseen trends. For instance, matches uncovering multiple cases of forced labor in the construction industry might instigate outreach efforts toward construction companies and local governance boards.

Expanding the Pilot

Working on this type of data showcases the power of Conclave for detecting shared patterns across cases. The pilot relies on a Secure Matching engine based on Conclave and R3 Corda nodes hosted by Hope for Justice to prove the concept of record matching and case collaboration. Eventually, each organization would host its own Corda node for collaboration, as shown in Figure 2.

As a pilot, this project is just one small step toward a more comprehensive use of the power of Confidential Computing to fight slavery—but it's an important step, one that will help verify that highly sensitive data can be shared more securely. Intel, R3, and Hope for Justice are optimistic that efforts such as this can truly lead to better lives for human beings in the future.

> "Human traffickers are exploiting new technology and globalisation at a staggering scale and pace. Most trafficking is now facilitated via the Internet and other digital technologies that pay little attention to borders or jurisdictions. We cannot lose the technology race against human trafficking.
>
> That is why we are so pleased that the Private Data Exchange platform has the potential to revolutionise how the sector collaborates across borders and overcomes issues surrounding data privacy and confidentiality. For the first time, civil society, governments, UN agencies and businesses can truly collaborate to make technology a force that will help to end human trafficking."
>
> *Tim Nelson, CEO, Hope for Justice*

R3

R3 is a leading provider of enterprise technology and services that enable direct, digital collaboration in highly-regulated industries where trust is a critical requirement. Conclave from R3 provides organizations both large and small with the tools needed to protect their data. With Conclave, organizations can prove to customers that critical code and data remain protected at all times.

Whether an organization needs to build Confidential Computing applications or scale workloads to meet increasing demands, Conclave delivers the tools needed to develop and host privacy-first applications and services.

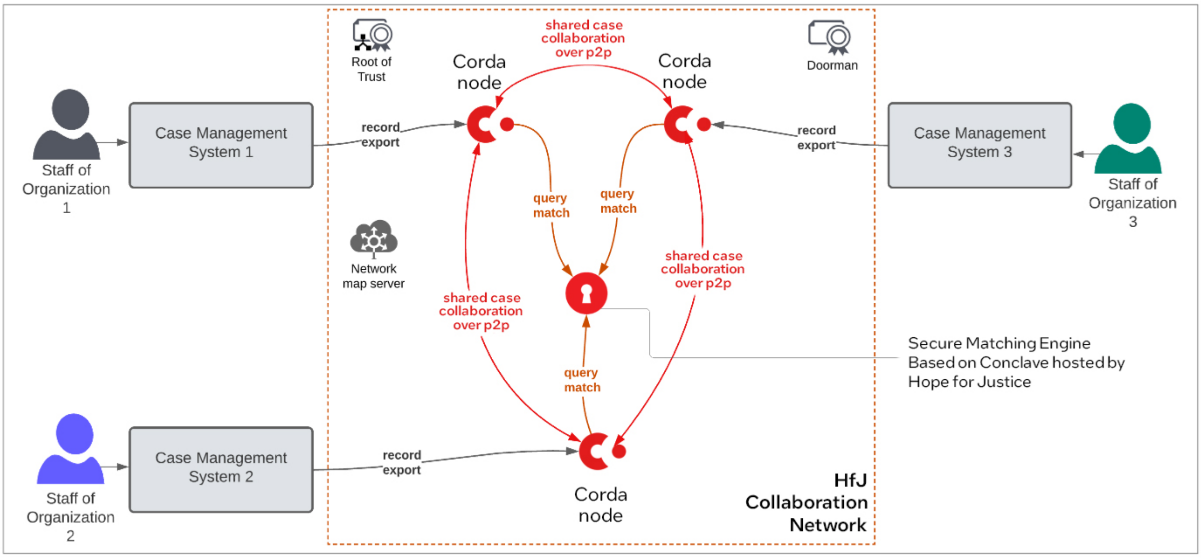

Figure 2: Sharing via multiple case management systems

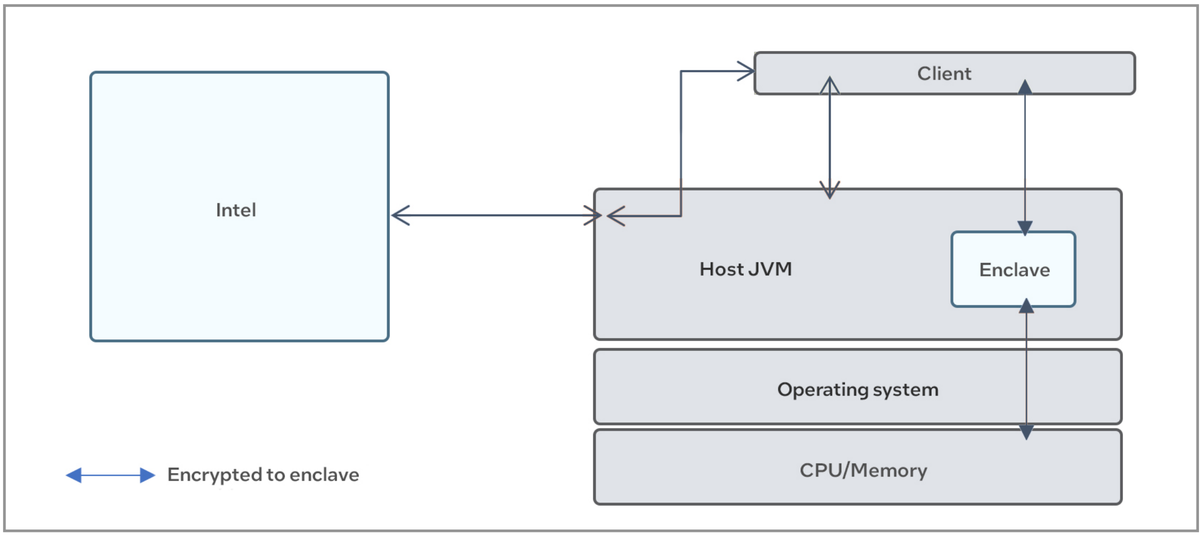

Figure 3: Secure Conclave Core enclaves run on TEEs protected by Intel SGX

Conclave Core

Conclave Core is an open-source software development kit (SDK) that enables the rapid development of privacy-preserving applications. With the Core SDK, developers can create Intel SGX enclaves using high-level languages such as Java, Kotlin, and JavaScript. It has a simple but powerful high-level API that hides the low-level complexities of using Intel SGX, so developers can spend more time concentrating on the enclave's business logic. The Core SDK also powers Conclave Cloud, R3's privacy-preserving SaaS platform for deploying confidential, event-driven workloads in the cloud.

Conclave Cloud

Conclave Cloud is a serverless Confidential Computing platform with built-in privacy-preserving features leveraging Intel SGX. Built on R3's Conclave Core SDK, Conclave Cloud provides the tools necessary to ensure data remains encrypted while in use and can only be shared with authorized parties. It provides organizations with a fast and easy way to build more secure applications. With Conclave Cloud, developers can host, execute, and scale stateless functions on demand. Organizations can run code without the burden of managing complex infrastructure, and focus on the development of functionality for improved time-to-value. Using Intel SGX, it keeps data fully encrypted at each stage of the data lifecycle.

All In all, Conclave enables ease and accessibility for those looking at harnessing the power of Intel SGX.

CONFIDENTIAL COMPUTING CONSORTIUM

Intel and R3 are members of the Confidential Computing Consortium, a leading force in advanced data security around the world.

Industry-leading Intel Technologies

The Intel-R3-Hope for Justice pilot takes advantage of the industry-leading security capabilities delivered by Intel SGX, the set of security features built into 3rd and 4th generation Intel® Xeon® Scalable processors. Designed specifically to support trusted computation, Intel SGX enables developers to partition code into hardened enclaves. Data processed inside an enclave is not accessible to other applications, the operating system, or hypervisor.

The combination of R3 aggregation features and the power and functionality of Intel technology opens new possibilities for organizations seeking to benefit from the security of confidential cloud computing. Intel technology can serve as the critical link, bringing together widely dispersed data so organizations can extract the previously inaccessible value hidden in it.

Intel's Purpose

We create world-changing technology that improves the life of every person on the planet. Find out more about Intel's corporate responsibility commitment: https://www.intel.com/content/www/us/en/corporate-responsibility/corporate-responsibility.html

Learn more

Hope for Justice
https://hopeforjustice.org

Hope for Justice Annual Review
https://hopeforjustice.org/annual-review/

R3
https://R3.com

R3 Conclave
https://www.conclave.net

Intel® Confidential Computing
https://www.intel.com/content/www/us/en/security/confidential-computing.html

Intel® SGX
https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

Intel® Xeon® Scalable processors
https://www.intel.com/content/www/us/en/products/details/processors/xeon/scalable.html

NOTICES AND DISCLAIMERS

[1] Hope for Justice UK=Modern-Slavery=Human-Trafficking-Briefing=Document-June-2022.pdf. See https://hopeforjustice.org/resources-and-statistics/resources-facts-figures/.

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure. Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.