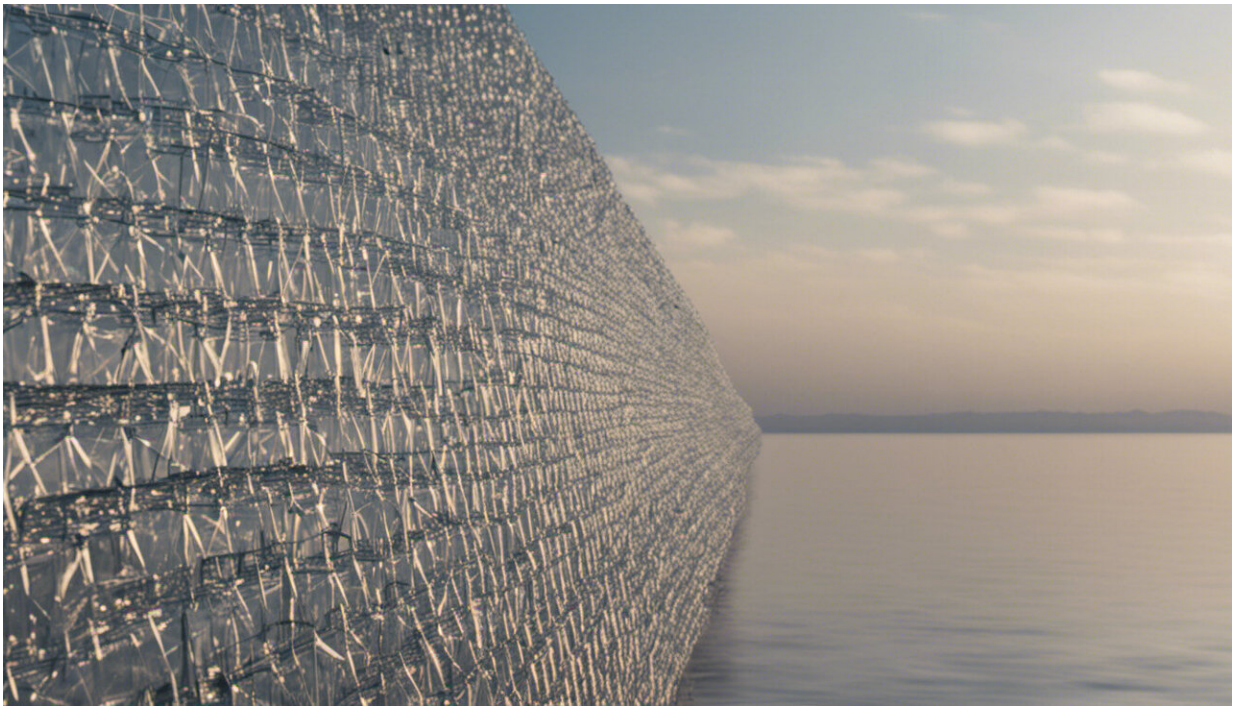
There are systems 'guarding' your data in cyberspace, but who is guarding the guards?

May 27 2022, by Joanne Hall, Geetika Verma and Matthew P. Skerritt



Credit: AI-generated image (disclaimer)

We use internet-connected devices to access our bank accounts, keep our transport systems moving, communicate with our colleagues, listen to music, undertake commercially sensitive tasks—and order pizza. Digital security is integral to our lives, every day.

And as our IT systems become more complex, the potential for vulnerabilities increases. More and more organizations are being breached, leading to financial loss, interrupted supply chains and identity fraud.

The current best practice in secure technology architecture used by major businesses and organizations is a "zero trust" approach. In other words, no person or system is trusted and every interaction is verified through a central entity.

Unfortunately, absolute trust is then placed in the verification system being used. So breaching this system gives an attacker the keys to the kingdom. To address this issue, "decentralization" is a new paradigm that removes any single point of vulnerability.

Our work investigates and develops the algorithms required to set up an effective decentralized verification system. We hope our efforts will help safeguard digital identities, and bolster the security of the verification processes so many of us rely on.

Never trust, always verify

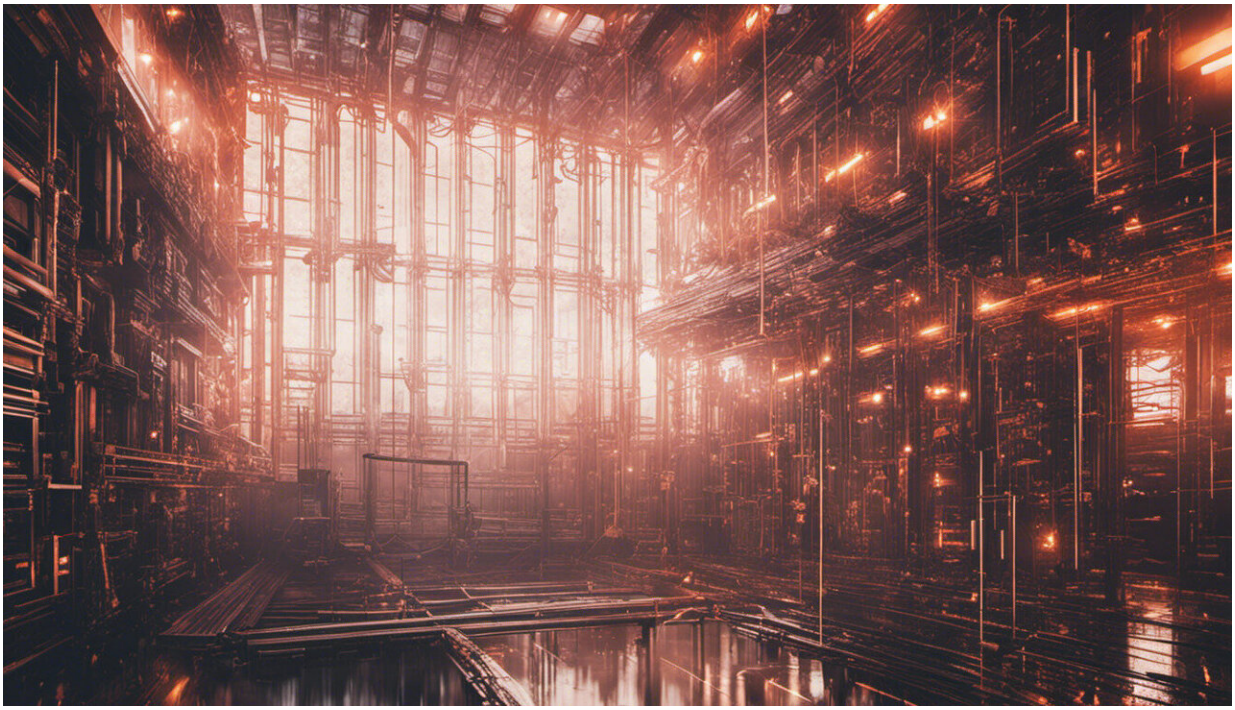
A zero trust system implements verification at every possible step. Every user is verified, and every action they take is verified, too, before implementation.

Moving towards this approach is considered so important that U.S. President Joe Biden made an executive order last year requiring all US federal government organizations to adopt a zero trust architecture. Many commercial organizations are following suit.

However, in a zero trust environment absolute faith is (counter intuitively) placed in the validation and verification system, which in

most cases is an Identity and Access Management (IAM) system. This creates a single trusted entity which, if breached, gives unencumbered access to the entire organizations systems.

An attacker can use one user's stolen credentials (such as a username and password) to impersonate that user and do anything they're authorized to do—whether it's opening doors, authorizing certain payments, or copying sensitive data.



Credit: AI-generated image (disclaimer)

However, if an attacker gains access to the entire IAM system, they can do anything the system is capable of. For instance, they may grant themselves authority over the entire payroll.

In January, identity management company Okta was hacked. Okta is a single-sign-on service that allows a company's employees to have one password for all the company's systems (as large companies often use multiple systems, with each requiring different login credentials).

When Okta was hacked, large companies who use their services, including FedEx, were concerned their accounts could be compromised. The attacker accessed some data, but did not gain control over any accounts.

Decentralizing trust

In our latest work, we refined and validated algorithms that can be used to create a decentralized verification system, which would make hacking a lot more difficult. Our industry collaborator, TIDE, has developed a prototype system using the validated algorithms.

Currently, when a user sets up an account on an IAM system, they choose a password which the system should encrypt and store for later use. But even in an encrypted form, stored passwords are attractive targets. And although multi-factor authentication is useful for confirming a user's identity, it can be circumvented.

If passwords could be verified without having to be stored like this, attackers would no longer have a clear target. This is where decentralization comes in.

Instead of placing trust in a single central entity, decentralization places trust in the network as a whole, and this network can exist outside of the IAM system using it. The mathematical structure of the algorithms underpinning the decentralized authority ensure that no single node that can act alone.

Moreover, each node on the network can be operated by an independently operating organization, such as a bank, telecommunication company or government departments. So stealing a single secret would require hacking several independent nodes.

Even in the event of an IAM system breach, the attacker would only gain access to some user data—not the entire system. And to award themselves authority over the entire organization, they would need to breach a combination of 14 independently operating nodes. This isn't impossible, but it's a lot harder.

But beautiful mathematics and verified algorithms still aren't enough to make a usable system. There's more work to be done before we can take decentralized authority from a concept, to a functioning network that will keep our accounts safe.

More information: *Correction: this article was updated to reflect that, while the Okta data breach gave hackers access to certain data, follow-up investigations found they did not gain control over clients' systems.*

Provided by The Conversation