MIT Lincoln Laboratory

# Success of MIT-LL's cloud server security technology now includes endorsement from tech giant IBM

## MIT Lincoln Laboratory

In just six years, a cloud security technology developed at MIT Lincoln Laboratory has evolved from an internal project to a key player in maintaining the security of IBM's thousands of cloud servers.

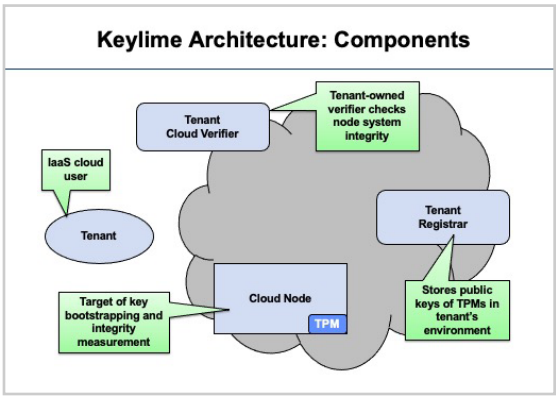
Keylime is a free, open-source security software architecture designed to help government and industry users with sensitive data protect their cloud and Internet of Things (IoT) devices. The system allows users to securely bootstrap secrets (securely upload cryptographic keys, passwords, and certificates) into the cloud without divulging them to a cloud provider and to continuously verify trust in their cloud computing resources without relying on a provider to do it for them.

In July 2021, IBM announced that it would be rapidly rolling out Keylime based technology to its entire cloud fleet to meet the security needs of its customers in financial services and other enterprise areas. This will leverage work done to expand the scalability and resilience of Keylime for managing large quantities of data, allowing Keylime to be applied across a cloud data center.

Keylime achieves its cloud security by leveraging a piece of hardware called a TPM (Trusted Platform Module), an industry-standard hardware security chip. A TPM generates a hash, a short string of numbers representing a much larger amount of data, that changes significantly if data are even slightly tampered with. Keylime can detect and react to this tampering in under a second.

Before Keylime, TPMs were incompatible with cloud technology, slowing down systems and forcing engineers to change software to accommodate the module. Keylime gets around these problems by serving as a piece of intermediary software that allows users to leverage the security benefits of the TPM without having to make their software compatible with it.

Keylime started as an internal project funded through MIT Lincoln Laboratory's Technology Office in 2015. Through the Massachusetts Open Cloud initiative, the




*Above: The Keylime system allows users to securely bootstrap secrets (securely upload cryptographic keys, passwords, and certificates) into the cloud without divulging them to a cloud provider.*

Keylime team began discussions with RedHat, one of the world's largest open-source software companies, to expand the technology's commercial reach.

With the help of RedHat and the Department of Homeland Security Science & Technology Directorate's Transition to Practice Program, the Keylime team developed an open-source distribution strategy that would facilitate updates to public and government systems. RedHat also helped Keylime to transition in 2019 into the Cloud Native Computing Foundation as a sandbox technology with more than 30 open-source developers contributing to it from around the world.

The Keylime community continues to attract members with diverse skill sets, experiences, and application interests. Through this diverse and growing community, Keylime is now:

- Available to be downloaded and installed from Fedora, a digital asset management content repository
- Being prepared for integration into the RedHat Enterprise Linux (RHEL) operating system as a trusted cloud integrity management security system
- Being re-implemented in the Rust operating system language for improved performance and safety.