

Genomic Data Security in the Cloud

INTRODUCTION

Data integrity and security are critical to the management of genomic data. The cloud offers on-demand scalability without the need to invest in capital equipment. However, due to its remote nature, there is general mistrust that cloud computing is actually secure. With its formation of the Life Informatics Center (LIC) and through its collaboration with [Google Cloud](#), HTA has developed a secure framework for the analysis and storage of genomic data.

THE LIC SECURITY FRAMEWORK

Along with data encryption, the [Google Cloud Platform](#) provides a cloud infrastructure with robust built-in compliance and security features applied to the physical datacenter, and the network. HTA has further built upon this infrastructure to create a secure platform for genomic data called the LIC Security Framework.

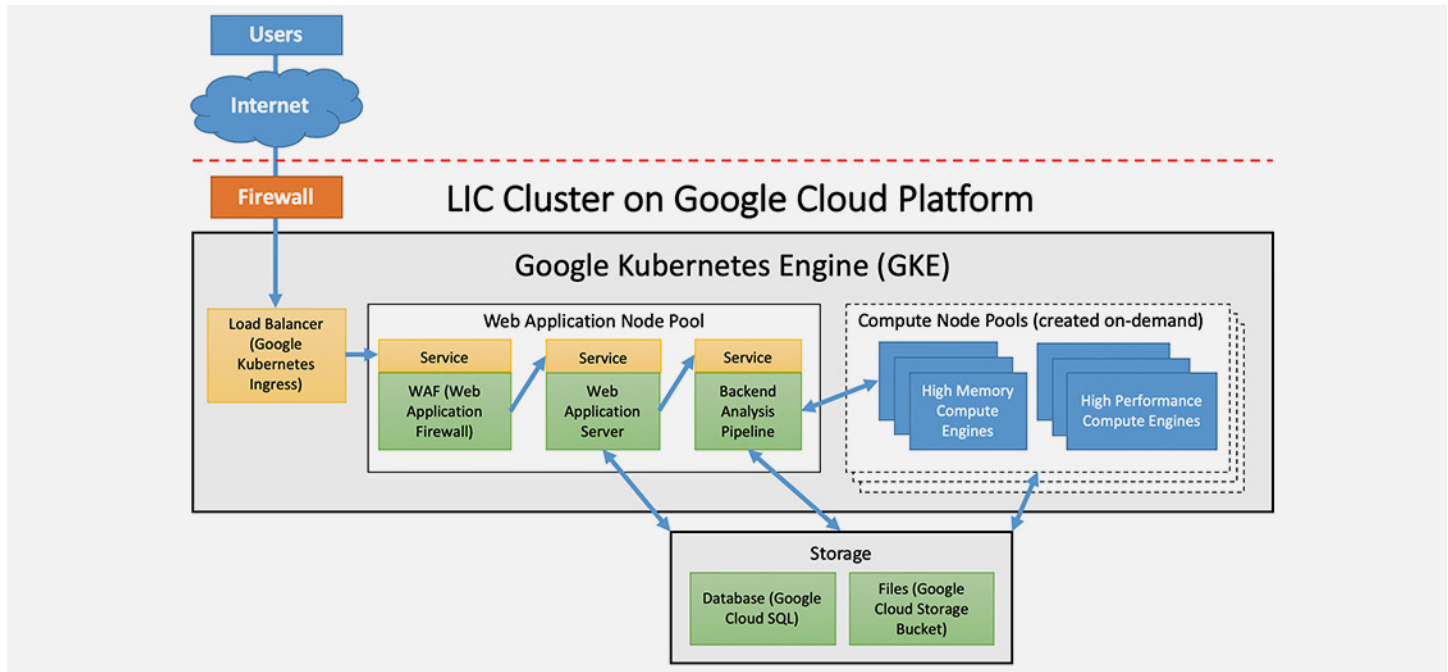
The cloud offers the dynamic scalability required for the storage and analysis of large genomic datasets, but the use of the cloud raises concerns about keeping this data secure. Hitachi High Technologies America, Inc. (HTA) has addressed these concerns without compromising accuracy or speed.

The LIC Security Framework includes the following:

- Protection against basic attacks (e.g. port scan, DDos, etc.) by the Google Cloud
- An additional security layer applied to the default Google Firewall, called the Web Application Firewall (WAF), to prevent more sophisticated attacks such as SQL injection attacks
- Storage (Database, Files) that is 100% Google Cloud based
- Google Cloud's full data encryption

[Human Chromosome Explorer](#) and [Microbial Explorer](#) are built on the LIC Security Framework.

The below diagram demonstrates the integration of the Google Kubernetes Engine and the LIC Cluster to form the LIC Security Framework



Attacks protected by each security component:

- **Google Firewall:** Port scan, IP/Port restriction, DoS/DDoS attacks
- **WAF:** SQL Injection, Cross-site scripting, Real-time application security monitoring, etc.

3. Audit log analysis and system-level inspection to identify suspicious behavior, potential attacks, or security breaches
4. A patch-management policy and scheduled server updates
5. Restriction of access for technical staff to resources on a per-need basis

LIC SECURITY FRAMEWORK (CONT.)

In addition to the security features described above, HTA has implemented the following best practices into the LIC Security Framework to both ensure stability and further enhance security.

1. Regular assessments to discover and remediate vulnerabilities
2. Regular penetration tests to discover vulnerabilities in the system that may not have been identified in the regular assessments

CONCLUSION

The cloud offers a powerful platform for the storage and analysis of genomic data. However, security and privacy concerns must be addressed. Through our partnership with Google Cloud, the LIC Security Framework brings trust to the platform. Finally, as security needs, concerns, and regulations will change and evolve, so will this framework. HTA is committed to security.