Using 'chaos engineering' to make cloud computing less vulnerable to cyber attacks

August 26 2024, by Amro Al-Said Ahmad

Credit: Pixabay/CC0 Public Domain

Cloud computing has emerged as a crucial element in today's technology, serving as the backbone for global connectivity. It empowers businesses, governments, and individuals to employ and construct cloud-based services and forms the foundation for a huge range of systems we use every day, including telecommunications, transportation, health care, banking, and even streaming services.

Such systems, like any hardware or software, are susceptible to failures

and cyberattacks that can occur unpredictably. Cybercriminals are becoming even more determined, and their attacks increasingly sophisticated and frequent. One of the tactics these groups frequently employ are distributed denial of service (DDoS) attacks, which flood companies' systems with more requests and traffic than their IT systems can handle.

This locks legitimate users out of the service, causing significant problems for companies, including revenue loss and diminished customer loyalty. This issue can cause major difficulties for companies like Google and Amazon, which offer cloud computing services to host consumers' data, systems, and services.

In our latest study, we employed several strategies to show how cloud computing systems can actually be strengthened by stress. We employed something called chaos engineering and adaptive strategies, which help the system learn from faults and cyberattacks.

In their most recent quarterly analysis of cybersecurity threats, cloud computing security company Cloudflare reported a 65% increase in DDoS attacks in the third quarter of 2023 compared to the previous quarter. According to Cloudflare's report for the second quarter of 2024, there were four million DDoS attacks.

Besides DDoS and other deliberate attacks, companies using cloud-based software are also vulnerable to outages caused by issues ranging from connection problems to physical server failures—some of which can also result from cyber-attacks. Sometimes, even a minor issue, such a typo, can knock cloud-based websites down.

On July 19 , crashes in CrowdStrike's Falcon sensor caused Windows hosts connected to the Microsoft Azure cloud computing system to crash, causing a global IT outage across the world.

The Falcon sensor, designed to prevent cyber-related attacks, was not compromised by a cyber-attack. The outage was caused by a technical issue with an update. On July 31, an error in Microsoft's DDoS defenses caused an eight-hour outage in Azure.

Unpicking fragility

Resolving major outages like these presents significant challenges due to the cloud's complexity and its many dependencies on other systems—including for cybersecurity. Implementing reliable fixes can take from hours to several days or, in some cases such as CrowdStrike's, even longer.

Such incidents demonstrate the fragility of our tech infrastructure in general, but particularly cloud-based systems. Solutions are currently focused on managing the effects of these incidents rather than addressing the root problems by creating more reliable and resilient cloud systems. To prevent failures, a crucial step is to integrate as standard, advanced tests of software to assess its resilience and dependability under pressure.

In our research, we're helping cloud consumers withstand these threats by doing exactly this, making cloud computing better able to withstand large attacks and outages and keep functioning. Those operating cloud systems also need to adapt and learn from previous incidents to make them stronger.

We have been using a technique called chaos engineering—deliberately attacking and experimenting with these cloud-based software applications—to look at how the system responds to such attacks.

One of our most recent papers found that we can use this technique to more accurately predict how a system will react to an attack. Chaos

engineering involves deliberately introducing faults into a system and then measuring the results. This technique helps to identify and address potential vulnerabilities and weaknesses in a system's design, architecture, and operational practices.

Methods can include shutting down a service, injecting latency (a time lag in the way a system responds to a command) and errors, simulating cyberattacks, terminating processes or tasks, or simulating a change in the environment in which the system is working and in the way it's configured.

In recent experiments, we introduced faults into live cloud-based systems to understand how they behave under stressful scenarios, such as attacks or faults. By gradually increasing the intensity of these "fault injections," we determined the system's maximum stress point.

Our investigation revealed a reduction in performance and the availability of services as a result. So these chaos engineering experiments uncovered issues that traditional performance measurements could not detect.

Learning from chaos

Chaos engineering is a great tool for enhancing the performance of software systems. However, to achieve what we describe as "antifragility"—systems that could get stronger rather than weaker under stress and chaos—we need to integrate chaos testing with other tools that transform systems to become stronger under attack.

In our latest work, we presented an adaptive framework to do exactly this. This framework, called "Unfragile," employs chaos engineering to introduce failures incrementally and assess the system's response under these stresses.

We then introduce new, adaptive strategies to eliminate the vulnerabilities found through chaos engineering. This can include modifying the source code of the software itself to improve its performance. By introducing metrics on the performance of the system in real-time, the system can become adaptive, as potential problems are picked up early and resolved.

By combining chaos engineering with these adaptive strategies to alert operators to vulnerabilities in real-time, so they can be fixed, we can teach cloud systems not only to withstand stress but to become stronger from it.

This will ensure that our critical digital infrastructure becomes more robust, reliable, and capable of learning from chaos to better confront future challenges.

Provided by The Conversation

Citation: Using 'chaos engineering' to make cloud computing less vulnerable to cyber attacks (2024, August 26) retrieved 27 August 2024 from https://techxplore.com/news/2024-08-chaos-cloud-vulnerable-cyber.html