# RESEARCH NEWS

**Preventing cyberattacks**

## Like a spellchecker for developers: automated detection of security vulnerabilities in cloud applications

**Cloud computing is a growing market. But cyberattacks on cloud software systems are on the rise, too, as these applications often contain security vulnerabilities that hackers are able to exploit. CodeShield software – which is produced by the company of the same name – uncovers these vulnerabilities and fixes them using automated methods. CodeShield is a spin-off of the Fraunhofer Institute for Mechatronic Systems Design IEM and the Heinz Nixdorf Institute at Paderborn University.**

More and more companies are moving their IT infrastructure to the cloud, using the storage and computing capacity offered by cloud services or programming applications directly in the cloud. Cloud systems offer numerous advantages, but they also require special security measures to be put in place. Many companies are unprepared for this — something which can have consequences for the security of their data. "Often, we see insecure web interfaces, incorrectly configured interfaces or vulnerable access protocols that are open to exploitation by cybercriminals. This can result in the loss of sensitive data, to name one example," states Prof. Eric Bodden, a scientist at Fraunhofer IEM. Together with colleagues from the Heinz Nixdorf Institute at Paderborn University, he established the spin-off CodeShield in 2020 and developed a tool of the same name that analyzes and evaluates the security of cloud applications and fixes vulnerabilities. In addition to Prof. Bodden, the start-up was founded by Manuel Benz, Andreas Dann and Dr. Johannes Späth and now has nine employees. "Targets of hacker attacks can include companies' publicly writable buckets. These types of cloud container store data in the form of objects. Attacks are possible if the bucket is not read-only and can therefore be accessed publicly, for example," explains Bodden. Well-known victims of this type of attack include trading platform BHIM and AutoClerk, a platform-based hotel property management system. The attacks resulted in millions of user and account data items falling into the hands of the perpetrators.

### Automatic detection of security vulnerabilities

The aim of CodeShield is to put a stop to these cybercrime activities. The software uses an automated process to analyze vulnerabilities in the program code, focusing on cloud-native applications, which are currently experiencing a boom in popularity. Prominent examples of cloud-native technologies include Spotify and Netflix. Electric scoot-

**Contact**
**Janis Eitner** | Fraunhofer-Gesellschaft, München, Germany | Communications | Phone +49 89 1205-1333 | presse@zv.fraunhofer.de
**Kirsten Harting-Stuke** | Fraunhofer Institute for Mechatronic Systems Design IEM | Phone +49 5251 5465107 | Zukunftsmeile 1 | 33102 Paderborn, Germany | www.iem.fraunhofer.de | kirsten.harting-stuke@iem.fraunhofer.de

ers, which have been a common sight on our streets for some time now, are also connected to the cloud. The applications are hosted directly by the cloud provider. The program code is also programmed in the cloud and is then is then stored and executed at companies such as Amazon Web Services, a popular provider in this field. The crux of the matter is as follows: "The interfaces and components made available by the providers – which can be described as a kind of modular toolbox – are not easy to use. Although they enable programmers to develop new applications within a short space of time, private data can end up being published inadvertently if the interfaces are configured incorrectly," says the computer scientist. "CodeShield doesn't just discover these vulnerabilities in real time using automated means – it also visualizes them at the same time." Covering everything from the website and app to the code and data container, the software presents the entire cloud infrastructure in the form of diagrams so that programmers can quickly identify problems and weaknesses. Components such as open-source libraries from third-party providers can also be integrated, displayed and checked here.

**Fingerprinting method and data flow analysis**

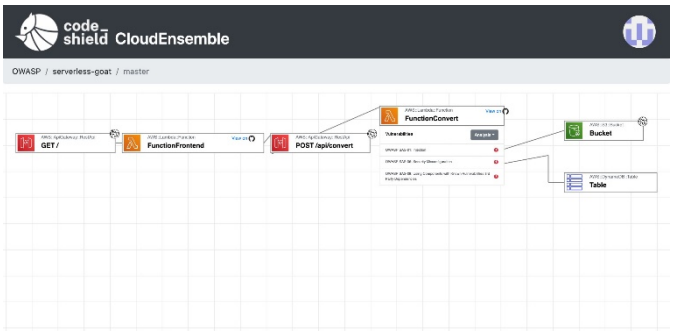
To uncover security vulnerabilities in the code, the tool uses what is referred to as a fingerprinting method. This involves Bodden and his team downloading the open-source components from the cloud and calculating a fingerprint for each component. This fingerprint enables any insecure code to be recognized immediately if it is integrated into an application again at a later date.

In addition, CodeShield analyzes the program code that developers write themselves, store in the cloud and constantly edit to adapt and expand functionalities. In this case, CodeShield conducts highly efficient dataflow analyses on a daily basis. The work of these analyses includes checking user inputs in the front-end to detect any manipulation quickly. Specially developed algorithms enable high-quality analyses to be conducted. CodeShield's false positive rate is below five percent. "Many IT security tools deliver false positives of between 70 and 80 percent, which is a huge problem for developers. That's comparable to a spellchecker that highlights errors in every sentence where there aren't any," explains the scientist. However, the CodeShield technology is different. As an example, it identified security vulnerabilities in Germany's coronavirus warning app before it was launched.

In 2019, CodeShield received the Ernst Denert Software Engineering Award.
CodeShield is funded by the European START-UP transfer.NRW program. CodeShield is also funded by the BMBF's StartUpSecure program.


**Picture 1 The CodeShield founding members: Dr. Johannes Späth, Prof. Dr. Eric Bodden, Manuel Benz, Andreas Dann (from left to right).**

**© CodeShield GmbH**




**Picture 2 CodeShield presents data flows in a clear visualization, enabling the level of threat to be assessed effectively.**

**© CodeShield GmbH**