ZERO TRUST TECHNOLOGY
APPLICATION FOR AI MEDICAL RESEARCH

Luchenko Y.V. Student of the Faculty of Computer Science
Kharkiv National University of Radio Electronics, Ukraine

Semenova V.V. Student of the Faculty of Computer Science
Kharkiv National University of Radio Electronics, Ukraine

Kravets N.S. Candidate of Technical Sciences, Associate Professor of the Department of Software Engineering,
Kharkiv National University of Radio Electronics, Ukraine

Summary. In this article, we briefly describe the relevance of introducing artificial intelligence into the healthcare sector. We point out the problems associated with the confidentiality of data and their collection when checking the performance of algorithms. We also talk about solving the problem in the form of a Zero Trust platform.

Keywords: Zero Trust technology, artificial intelligence, neural network, machine learning, Azure confidential computing, data set.

Artificial intelligence is being introduced into many spheres of human life. One of them is the health sector. The research firm Frost & Sullivan estimates that AI has the potential to improve patient outcomes by 30% to 40% while reducing treatment costs by up to 50% (Hsieh, 2017a) [1].

AI and machine learning can improve healthcare and reduce costs. For example:
- The use of neural network analysis of data on risk factors in comparison with the processing of information that forms a clinical picture allows the diagnosis of a potential disease with cholecystitis before the onset of symptoms [2];
- Two IBM Watson Health clients recently found that with AI, they could reduce their number of medical code searches by more than 70% [3];
- A team from MIT’s Computer Science and Artificial Intelligence Laboratory (CSAIL) and Massachusetts General Hospital (MGH) has created a new deep-learning model that can predict from a mammogram if a patient is likely to develop breast cancer as much as five years in the future [4].
The effectiveness of the implementation of artificial intelligence is high, but a large amount of data is needed to train it. This is where the confidentiality problem arises. Thus, according to the results of 2019, out of more than 12,000 biomedical scientific papers, AI and machine learning were described [5], but only up to 40 of them received aFDA approval [1].

Since medicine requires high reliability from technologies, they should be unpretentious in the quality of input data. For example, benign moles can be perceived as cancerous due to noise in the images. Finding and fixing such problems requires a lot of training data. But at the same time, developers cannot get access to all the necessary data, since they are confidential.

The concept of Zero Trust can help deal with this problem. It is based on the principles:

- verify explicitly;
- use least privilege access;
- assume breach.

Zero Trust is implemented on three levels:

- Hardware. At this level, network micro-segmentation is performed. This requires the use of network devices such as a switch, firewall, or another gateway device. As a result, individual resources or groups of resources are on their own protected network segment.

- Software. This is where the software-defined perimeter is created. Software-Defined Networks (SDN) and intent-based networking (IBN) are often used for these purposes. As a result, the gateway is deployed at the application level. This gateway establishes a secure channel between the user and the resource.

- Organizational. At this level, administrators create and assign user roles and permission sets for them.

Across the Zero Trust journey, capabilities can be built and integrated to ‘unlock’ a series of benefits – from decreasing cyber risk and improving user experience to reducing IT costs and enabling better digital collaboration [6]. For this reason, the technology is successfully applied or is being introduced in the following areas:

- Internet of Things. This model covers a significant portion of the key things such as device access control, network access control, visibility & analysis, automatic security, data control, user control, workloads, etc [7].

- Supply chain management. The Zero Trust approach allows influencing important aspects of supply chain management including sustainability, corruption, counterfeit materials and products, and low quality practices that can hurt the reputations of organizations [8].

- US federal agencies. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The US government believes that the implementation of the Zero Trust approach will help to cope with the problems that have arisen [9].

As in the above areas, the Zero Trust model is great for medical research. Especially due to the second principle - the implementation of access based on roles. This is ideal for medical research, as developers do not need to access to specific data instances to test the success of the algorithms.
Building on this, UCSF with the support of Microsoft, Intel and Fortanix has implemented a zero-trust platform for AI research in medicine. This platform is called BeeKeeperAI. The idea is that the owner of the algorithm does not have access to the data network, the owner of the data does not have access to the algorithm, and the platform does not have access to either the data or the algorithm.

BeeKeeperAI provides the following functionality:
- Protected cloud storage which eliminates the loss of control and “resharing” risk;
- Encryption of primary data for their protection;
- Healthcare-specific tools & workflows which support data set creation, labeling, segmentation, and annotation activities;
- Complete data protection with Secure Enclave technology;
- Mediation between data stewards and algorithm developers.

Thanks to this approach, developers save time, effort and project costs by working with specially prepared data sets. They do not need to worry about compliance with the law, data retrieval and the formation of datasets in accordance with certain characteristics.

A combination of hardware and software technologies was used to create the platform. BeeKeeperAI is accessed through Azure Confidential Computing (figure 1). Azure Kubernetes Service (AKS) hosts confidential computing nodes. Azure Attestation establishes trust with the diagnostic provider. Hospital data is not available to the diagnostic provider because using this Azure components, the architecture isolates confidential patient data, and specific general data is processed in the cloud [10].

![Azure Confidential Computing architecture](image)

Fig. 1. **Azure Confidential Computing architecture** [10]

The hardware on which the virtual machines run is based on Intel processors with Intel Software Guard Extensions (SGX) technology. Intel SGX encrypts and isolates algorithms and data within enclaves, which are protected parts of the processor and memory. Fortanix software is responsible for encryption and control of worker processors.

BeeKeeperAI works in several stages [11]:
1. Receives an encrypted algorithm from the owner;
2. Wraps the algorithm in a secure compute container;
3. The algorithm is transferred to a secure encrypted environment of the data owner, in which the calculations will take place;
4. The data and algorithm are brought together. The algorithm runs and returns the values;
5. Secure computing enclave returns a confidential performance report and the general characteristics of the data set it ran against;
6. Finally, the data and algorithm are destroyed.

As a result, all property remains confidential, but developers have access to the exact results of their algorithms.

Thanks to the introduction of this platform, the development of medical technologies will be able to reach a new level. The platform will become available in March 2022.

**Conclusion.** In this article, we have described the relevance of using Zero Trust in various fields of activity. We also indicated the prospects for the development of medical artificial intelligence using the principles of this model.

**References:**


