deep learning models and deep learning will become faster and less resource-intensive.

References

1. What is Deep Learning? and What are its Significance? // AALPHA [Web-site]. URL: https://www.aalpha.net/blog/what-is-deep-learning-and-what-are-its-significance/

2. What Is Deep Learning and How Does It Work? // builtin [Web-site]. URL: https://builtin.com/machine-learning/deep-learning

3. Deep learning architectures // IMB Developer [Web-site]. URL: https://developer.ibm.com/articles/cc-machine-learning-deep-learning-architectures/

## SECURING YOUR AWS WORKLOADS: BEST PRACTICES FOR IDENTITY AND ACCESS MANAGEMENT

*Semko D., student,*

*Gerasymchuk T.V., Associate Professor,*

*Kharkiv National University of Radioelectronics*

As more organizations move their IT infrastructures to the cloud, Amazon Web Services (AWS) has become a leading provider of cloud computing services. AWS offers a range of services, including storage, compute, and database management, that allow organizations to quickly scale their resources and meet their business needs.

However, with the benefits of cloud computing come unique security challenges, particularly when it comes to Identity and Access Management (IAM).

IAM is a critical component of securing AWS workloads. Organizations must ensure that only authorized users have access to their resources and that those users are granted the appropriate level of access.

The least privilege principle is a security best practice that restricts user access to only the resources and data necessary for their job functions. By limiting user access, organizations can reduce the risk of insider threats and unauthorized access to sensitive data. IAM policies, which we can define as a set of rules that define the permissions granted to AWS users, should be designed with the least privilege principle in mind to ensure that users only have the necessary permissions to perform their tasks. AWS

offers various IAM policies, such as roles and groups, that can be used to implement the least privilege principle [1].

One of the most important IAM best practices is to use multi-factor authentication [3]. MFA requires users to provide more than one form of authentication to access their AWS resources. This can include something the user knows (such as a password), something the user has (such as a security token), or something the user is (such as a biometric identifier). IAM policies should include

MFA for privileged users, such as administrators and developers, to protect AWS resources from unauthorized access. AWS offers various MFA options, including hardware tokens, virtual MFA devices, and SMS text messages [1].

Another important IAM best practice is to use role-based access control (RBAC). RBAC allows organizations to grant access to resources based on a user's job function, such as administrator, developer, or analyst. These roles can then be assigned to users, allowing them to access only the resources necessary for their job function. This can help to simplify the management of user accounts and access privileges, while also reducing the risk of unauthorized access. AWS provides various

RBAC options, including IAM roles and AWS Organizations, which can be used to implement RBAC policies [1].

Regular auditing and monitoring of access logs is also critical for securing AWS workloads. Access logs record all actions performed on AWS resources, including successful and failed attempts to access resources.. By monitoring access logs, organizations can quickly detect and respond to potential security threats, such as brute-force attacks or unauthorized access attempts. AWS offers various monitoring and auditing tools, including CloudTrail and CloudWatch, which can be used to monitor and audit access logs [2].

In conclusion, securing AWS workloads requires careful planning and implementation of best practices for IAM. By using multi-factor authentication, role-based access control, and regular auditing and monitoring, organizations can reduce the risk of unauthorized access and maintain strong security posture in the cloud. As cloud

computing continues to grow in popularity, it is important for organizations to prioritize security and take proactive steps to protect their sensitive data.

References

1. AWS Security Best Practices / Jeff Barr – Amazon Web Services, 2018 – 76 p.
2. Implementing Identity Management on AWS / Lehtinen J. – Packt Publishing, 2021 – 504 p.
3. Cloud Computing Security: Foundations and Challenges / John R. Vacca – CRC Press, 2020 – 522 p.

## BLOCKCHAIN TECHNOLOGY. DLT.

*Priadko V. S., student*
*Gerasymchuk T. V., Associate Professor*
*Kharkiv National University of Radio Electronics*

Today, few people can say they have never encountered, or at least heard of, blockchain or cryptocurrencies; those who can, are usually envied. Years of blockchain technology development in one direction - cryptocurrencies - and the monopolization of the cryptographically-secure distributed networks market by blockchains have shaped a firm thesis in the average observer: blockchain equals cryptocurrencies. Of course, part of this is true, almost always cryptocurrencies are built within the framework of one or several blockchains, but not all blockchains are created to bring one more value bearer into the world.

Blockchain is one of the ways to implement distributed ledger technology. A distributed ledger is one of the types of P2P networks in the first financial-economic approximation. Blockchain is not a separate technology that was created to deceive people for the purpose of enrichment, but rather a logical product of progress and work of scientists and engineers.

After the collapse of several centralized crypto exchanges, recent breaches of popular protocols (products that are entirely or partially built on the basis of blockchain), and the bankruptcy of some American banks, Western society, which had previously been rather unsympathetic to the decentralization of the financial system,