Impact Factor: 9.9 ISSN-L: 2544-980X

CREATING METHODS TO PREVENT CYBERATTACKS IN CLOUD ENVIRONMENTS.

Samatova Zarnigor Nematovna
2nd year master's student ,Tashkent University of Information Technologies, Fergana Branch
Email : rakhimovaz@mail.ru

Abstract: The article is aimed at creating methods for preventing cyberattacks in a cloud environment and analyzes modern approaches and mathematical models for cloud security. Cloud technologies are important in ensuring the security of corporate and personal data, but they require new approaches to protecting against cyberattacks. The article shows the importance of cloud backup and disaster recovery systems, and also analyzes mathematical models and algorithms for preventing cyberattacks in cloud systems, including approaches based on probability theory, statistical analysis, machine learning (ML), and artificial intelligence (AI).

Keywords: Cloud security, cyberattacks, mathematical models, algorithms, probability theory, statistical analysis.

Introduction

Cloud backup is an essential part of an effective cloud security program. It helps protect against threats such as ransomware and malware, as well as against accidental or malicious changes or sabotage to cloud assets. Cloud backup allows an organization to send a copy of files or entire systems (such as virtual machines or containers) to a cloud-based location. The copy is stored in a cloud data center and can be restored if the original data is lost. Cloud backup services typically charge based on the storage space used, data transfer bandwidth, and access frequency. They can be used to back up both on-premises and cloud-based resources.

Another important function of cloud backup is disaster recovery. Traditionally, disaster recovery involves creating an entire secondary data center and switching to it in the event of a disaster. This solution is expensive to deploy in a single organization and is out of reach for smaller organizations. Cloud disaster recovery solutions are an attractive alternative, allowing organizations to easily deploy copies of their systems in the cloud and activate them on demand in the event of a disaster.

Methods

A cloud-native application is software designed to run on a cloud infrastructure. There are many definitions of cloud-native applications, and the term is often used interchangeably with microservices architecture. Cloud-native applications typically have the following characteristics:

Resilient - Cloud-native applications are able to handle failures as a normal event, without downtime or service interruptions.

Agile - cloud-native applications are developed using automated continuous integration / continuous delivery (CI/CD) processes and are composed of small, independent components that can each be developed and updated rapidly.

Efficiency - Cloud-native applications are easy to test, deploy, and manage. They have advanced automation that manages system components throughout all stages of the lifecycle.

Observable - Cloud native applications easily expose information about application status, failures. Each component in the system is responsible for generating meaningful logs to provide insight into its performance.

Impact Factor: 9.9 ISSN-L: 2544-980X

In the field of cybersecurity, the creation of methods for preventing cyber attacks in a cloud environment is gaining great importance along with the development of modern technologies and data exchange. Although cloud technologies have expanded the possibilities of storing, processing and sharing corporate and personal data, the problems of ensuring their security are also increasing. As cyber attacks become increasingly complex and traditional protection methods are insufficient, the development of new scientific approaches, mathematical models and algorithms is required. Below, the processes of creating mathematical models and algorithms for preventing cyber attacks in a cloud environment, testing them through experiments and analyzing the results through graphs are considered in detail.

Cybersecurity issues in cloud environments are mainly focused on ensuring the confidentiality, integrity, and availability of data. Data wide on a scale spread and virtual resources dynamic nature because of traditional security measures enough For example , Distributed Denial of Service (DDoS) attacks can theft , harmful programs (malware) and users personal information break such as threats cloudy in the environment wide spread . Such attacks prevent to take for complicated mathematician models and algorithms working exit necessary .

Results

Cloudy in the environment cyberattacks determination and prevent to take for various mathematician models are used . These between probability theory , statistics analysis , machine machine learning and artificial artificial intelligence (AI) based models important place Below this models main aspects and their application seeing is released .

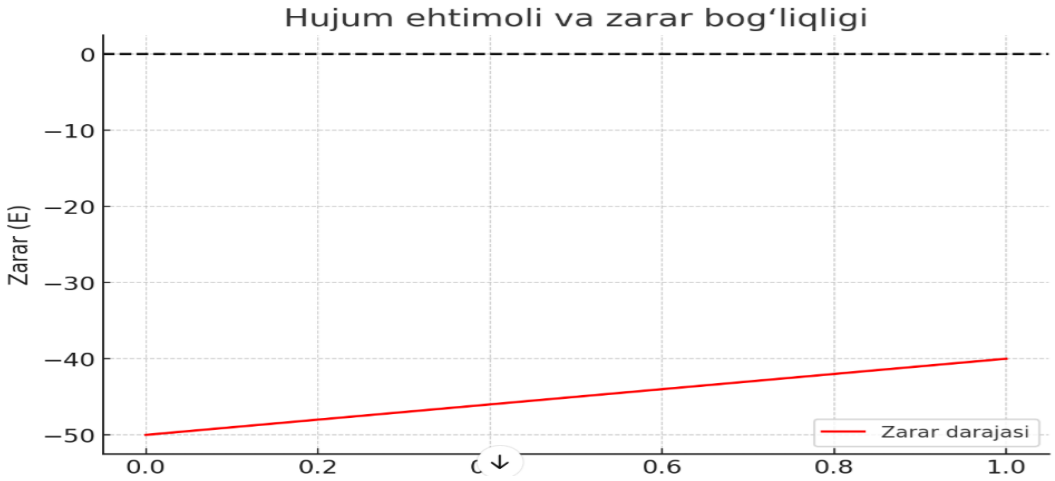

Figure 1. Attack probability and damage connection .

Probability theory based on cyberattacks determination for information flow statistic in terms of analysis to do For example , the network normal and abnormal traffic movements distinction for probability distributions Poisson distribution using network packages arrival frequency modeling If the packages arrival speed known one from tmhe border If it increases , it is a DDoS attack . sign to be possible .

Mathematician in terms of , Poisson distribution with the following formula is expressed as :

$$P(X = k) = \frac{\lambda^k e^{-\lambda}}{k!}$$

Here:

λ – average number of events,

k – number of observed events,

e is the base of the natural logarithm.

Impact Factor: 9.9 ISSN-L: 2544-980X

Statistical analysis can measure how much a data stream deviates from a normal distribution to detect anomalous behavior. If the deviation exceeds a certain threshold, it is considered a sign of a cyberattack.

Machine learning (ML) and artificial intelligence (AI) technologies are widely used in detecting and preventing cyberattacks. ML algorithms can analyze large amounts of data and identify abnormal behavior. For example, algorithms such as Support Vector Machines (SVM), Neural Networks, and Decision Trees are effective in detecting cyberattacks.

The SVM algorithm is used to solve two-class classification problems. This algorithm aims to separate the data with the highest margin. Mathematically, the SVM solves the following optimization problem:

$$\min_{w,b} \frac{1}{2}\|w\|^2 \text{with condition} y_i(w \cdot x_i + b) \geq 1, \forall i$$

Here:

w is the vector normal,

b – displacement parameter,

x_i – data point,

y_i – categories (1 or -1).

Neural networks, on the other hand, are used to study large amounts of data and identify complex patterns. They can be used to detect abnormal behavior in network traffic.

Experiments were conducted to test the created mathematical models and algorithms. Experiments for real cloudy in the environment taken information dataset used . Data The set includes normal and abnormal movements. own inside Experiences as a result following results taken :

Probability theory based model: Poisson distribution DDoS attacks using 85 % accuracy in detection However , this model is different . kind of attacks in determining not much effective it's not .

Machine-made education algorithms : SVM algorithm 92% accuracy using result taken from . Neuron networks and 95% accuracy to the index achieved . These results with car education algorithms cyberattacks in determining high efficiency shows .

Experiments the results to describe for following graphs compiled :

Accuracy Chart : Various algorithms accuracy indicators compared . Neuron networks the most high accuracy showed .

Table 1.Accuracy percent .

Algorithm	Accuracy (%)
Probability Model	85
SVM	92
Neuron networks	95

Error Level (Error Rate) Graph : Probability theory based on in the model mistake level high if yes , by car to teach in algorithms this indicator low was .

Table 2. Error level .

Algorithm	Error Level (%)
Probability Model	15
SVM	8
Neuron networks	5

Impact Factor: 9.9
ISSN-L: 2544-980X

Performance Execution Time Graph : Neuron networks other to algorithms relatively more takes time , but their accuracy level high .

Table 3. Performance time .

Algorithm	Performance Time (seconds)
Probability Model	2
SVM	5
Neuron networks	10

Conclusion

Cloudy in the environment cyberattacks prevent to take for mathematician models and algorithms working exit modern cybersecurity the most important from directions is one . Probability theory , statistics analysis , machine education and artificial intellect based on approaches cyberattacks determination and prevent in receiving high efficiency Showing . Experiments results this It turns out that the machine teaching algorithms , in particular neuron networks , cyberattacks in determining the most high accuracy provides . In the future this models further improvement and them real cloudy in the environment application cybersecurity further reinforcement opportunity gives .

References

1. Zulunov R., Samatova Z., Cyber security problems and methods of ensuring it. Descendants of Al-Fargani, 2024, 1(2), 322–326
2. Zulunov R., Samatova Z., CASB solutions in ensuring cybersecurity in cloud technologies Potomki Al-Fargani, 2024, 1(1), pp. 93–98.
3. R. Zulunov. Technology of robotic process automation in medicine. Potomki Al-Fargani, 2024, 1(4), 197-200.
4. R.Zulunov, M.Sattarov. Healthcare automation: a way to improve patient experience. Descendants of Al-Fargani, 2024, 1(2), 189–195.
5. R. Zulunov, O. Meliboev. Sovremennye realii umnoy meditsiny dlya studentsov. Miasto Przyszłości, 2024, T-48, c. 1052-1055.
6. R.Zulunov. Building and predicting neural networks in Python. Al-Farghaniy Avdollari, 2023, 1/4, p. 22-26.
7. R Zulunov, O Otakulov. Ogranicheniya obucheniya zyzyku programming JAVA v obrazovatelnyx sistemax. Potomki Al-Fargani, 2023, t.1/2, p. 37-40 .
8. R Zulunov. M Mahmudova. Electronic queue system in medical institutions. Descendants of Al-Fargani, 2023, 1(2), p. 53-57
9. R. Zulunov, A. Kayumov. Identification and sorting of textiles for automated processing with auxiliary infrared spectroscopy . Universum: tekhnicheskie nauki, 3(120), March 2024, p. 38-42 .
10. R. Zulunov, B. Soliev. Z. Ermatova. Enhancing Clarity with Techniques for Recognizing Blurred Objects in Low Quality Images Using Python. Potomki Al-Fargani, 2024, 1(2), 336–340.
11. VV Byts', RM Zulunov. Specification of matrix algebra problems by reduction. Journal of Mathematical Sciences. T. 71, 2719–2726 (1994).

Impact Factor: 9.9 ISSN-L: 2544-980X

12. Hnatiienko, H., Hnatiienko, V., Zulunov R., Babenko, T., Myrutenko, L. Method for Determining the Level of Criticality Elements when Ensuring the Functional Stability of the System based on Role Analysis of Elements . CEUR Workshop Proceedings , 2024, 3654, p. 301–311
13. R. Zulunov, B. Soliyev, A. Kayumov, M. Asraev, Kh. Musayev, D. Abdurasulova. Detecting mobile objects with ai using edge detection and background subtraction techniques . E3S Web of Conferences , 508, 03004 (2024).
14. R. Zulunov, U. Akhundzhanov, B. Soliyev, A. Kayumov, M. Asraev, Kh. Musayev. Building and predicting a neural network in PYTHON . E3S Web of Conferences , 508, 04005 (2024).
15. U. Akhundzhanov, R. Zulunov, A. Kayumov, H. Goipova, Z. Ermatova, M. Sobirov. Handwritten signature preprocessing for off-line recognition systems. E3S Web of Conferences 587, 03019 (2024), GreenEnergy 2024 .