МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК НА ХМАРНІ СИСТЕМИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро Кондратюк
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Дмитро КОНДРАТЮК
Ім’я, ПРІЗВИЩЕ

Керівник: Віталій ТИЩЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент:
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кондратюку Дмитру Олеговичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Застосування штучного інтелекту для захисту від кібератак на хмарні системи ”,
керівник кваліфікаційної роботи ТИЩЕНКО Віталій
(ІПРІЗВИЩЕ, Ім'я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “27“ лютого 2024 р. №36.

2. Строк подання кваліфікаційної роботи “ ” травня 2024р.
3. Вихідні дані до кваліфікаційної роботи: *кібербезпека, хмарні системи, штучний інтелект, методи та засоби захисту хмарних систем, нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література*..
4. Перелік питань, які мають бути розроблені:
   1. Проаналізувати основні види та особливості кібератак на хмарні системи.
   2. Дослідити роль штучного інтелекту у виявленні та запобіганні кібератакам на хмарні системи.
   3. Розробити рекомендації щодо впровадження штучного інтелекту для захисту хмарних систем від кібератак на основі досліджених методів та засобів.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “22“ лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання Етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	13.03.2024	
2.	Збір та аналіз літератури.	30.03.2024	
3.	Аналіз основних видів та особливостей кібератак на хмарні системи.	17.04.2024	
4.	Дослідження ролі штучного інтелекту у виявленні та запобіганні кібератак на хмарні системи.	01.05.2024	
5.	Розробка рекомендацій щодо впровадження штучного інтелекту для захисту хмарних систем від кібератак на основі досліджених методів та засобів	15.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	22.05.2024	
7.	Оформлення роботи.	24.05.2024	
8.	Оформлення презентації.	01.06.2024	
9.	Отримання рецензії на роботу.	04.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач(ка) вищої освіти _____ Дмитро КОНДРАТЮК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій ТИЩЕНКО _
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Кондратюку Д.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Застосування штучного інтелекту для захисту від кібератак на хмарні системи.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КОНДРАТЮК Дмитро у кваліфікаційній роботі проаналізував застосування штучного інтелекту для захисту від кібератак на хмарні системи, дослідив основні характеристики технологій штучного інтелекту для виявлення та реагування на кіберзагрози в хмарних середовищах, вивчив інструменти та методи оптимізації процесів виявлення та реагування на кібератаки за допомогою ШІ, а також розробив практичні рекомендації.

КОНДРАТЮК Дмитро показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на одній конференції. Все це дозволяє оцінити кваліфікаційну роботу здобувача КОНДРАТЮКА Дмитра на оцінку “_____” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи ____ Віталій ТИЩЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“_____“____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кондратюк Д.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти Кондратюка Дмитра
на тему "Застосування штучного інтелекту для захисту від кібератак на хмарні системи "

Актуальність. Сьогоднішній світ переживає значне зростання кількості кібератак на хмарні системи, що викликає потребу у вдосконаленні методів захисту інформації. Застосування штучного інтелекту для захисту від кібератак на хмарні системи є критично важливим завданням, оскільки ці системи зберігають великі обсяги чутливих даних та забезпечують функціонування багатьох організацій. Дослідження у цій сфері є надзвичайно актуальним і відповідає сучасним потребам у забезпеченні інформаційної безпеки, що дозволяє зменшити ризики втрат даних та фінансових збитків.

Позитивні сторони.

1. У роботі досліджено особливості використання штучного інтелекту для захисту від кібератак на хмарні системи.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.
3. Автор опрацював значну джерельну базу: близько 42 публікацій, в тому числі 30 англомовних.
4. За результатами дослідження запропоновано рекомендації щодо оптимізації процесів захисту від кібератак на хмарні системи за допомогою штучного інтелекту.

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для оцінки ефективності процесів захисту від кібератак на хмарні системи.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "_____", а здобувач Кондратюк Дмитро заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню проблем застосування штучного інтелекту для захисту від кібератак на хмарні системи. Робота складається зі вступу, трьох розділів, що містять 10 рисунків, висновків та списку використаних джерел, що містить 22 найменування. Загальний обсяг роботи становить 53 аркушів, з яких 3 аркуша займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження засад забезпечення інформаційної безпеки хмарних систем із застосуванням штучного інтелекту для захисту від кібератак. Для цього у роботі використовуються методи системного аналізу та теорії інформаційної безпеки, теорії штучного інтелекту та машинного навчання.

Об'єктом дослідження є забезпечення інформаційної безпеки хмарних систем.

Предмет дослідження - особливості застосування штучного інтелекту для захисту хмарних систем від кібератак.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, теорії інформаційної безпеки, теорії штучного інтелекту, а також методи машинного навчання та глибинного навчання.

Як результат у роботі проведено аналіз основних видів та особливостей кібератак на хмарні системи; досліджено сучасні методи та засоби захисту хмарних систем від кібератак з акцентом на використання штучного інтелекту; представлено схему взаємодії компонентів системи штучного інтелекту для захисту хмарних систем; досліджено ефективність використання методів машинного навчання та глибинного навчання для захисту хмарних систем від кібератак.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою хмарних

систем у контексті протидії загрозам, пов’язаним із кібератаками, зокрема із застосуванням штучного інтелекту для виявлення та запобігання таким атакам.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ХМАРНИХ СИСТЕМ, КІБЕРАТАКИ, ШТУЧНИЙ ІНТЕЛЕКТ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, МАШИННЕ НАВЧАННЯ, ГЛИБИННЕ НАВЧАННЯ.

ABSTRACT

The qualifying paper is dedicated to researching the issues related to the application of artificial intelligence for protecting cloud systems from cyber attacks. The work consists of an introduction, three chapters containing 10 figures, conclusions, and a list of references comprising 22 titles. The total volume of the paper is 53 pages, including 3 pages dedicated to the list of abbreviations and the list of references.

The objective of the paper is to explore the principles of ensuring the information security of cloud systems using artificial intelligence to protect against cyber attacks. To achieve this, the paper employs methods of systems analysis, information security theory, artificial intelligence theory, and machine learning.

The object of research is ensuring the information security of cloud systems.

The subject of research is the peculiarities of applying artificial intelligence to protect cloud systems from cyber attacks.

Research methods. To solve the aforementioned scientific task, the paper utilizes methods of systems analysis, information security theory, artificial intelligence theory, as well as machine learning and deep learning methods.

As a result, the paper provides an analysis of the main types and characteristics of cyber attacks on cloud systems; investigates modern methods and tools for protecting cloud systems from cyber attacks, focusing on the use of artificial intelligence; presents a scheme of interaction between components of the artificial intelligence system for protecting cloud systems; and examines the effectiveness of using machine learning and deep learning methods to protect cloud systems from cyber attacks.

Application area. The developed approaches can be used in the planning and implementation of an information security management system for cloud systems in the context of countering threats related to cyber attacks, particularly using artificial intelligence to detect and prevent such attacks.

Keywords: INFORMATION SECURITY OF CLOUD SYSTEMS, CYBER ATTACKS, ARTIFICIAL INTELLIGENCE, INFORMATION SECURITY MANAGEMENT SYSTEM, MACHINE LEARNING, DEEP LEARNING.

ЗМІСТ

ПРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ШІ - Штучний Інтелект

IT – Information Tecnology

DDoS - Distributed Denial-of-Service

IBM - International Business Machine

LOF - Local Outlier Factor

IP - Internet Protocol

IDS - Intrusion Detection System

IPS - Instructions Per Second

VPN - Virtual Private Network

RBAC - Role-Based Access Control

API - Application Programming Interface

SMS - Short Message Service

ПЗ - Прогамне Забезпечення

ВСТУП

Актуальність теми. У сучасному світі технології, зокрема штучний інтелект, стрімко розвиваються і все більше впливають на різні сфери життя та професії. Їх вплив важко переоцінити.

Штучний інтелект допомагає фахівцям з різних галузей, полегшуючи виконання рутинних завдань.

Очевидно, що спеціалісти з кібербезпеки не могли оминути увагою таку технологію. Дослідження Інституту Capgemini у 2018 році показало, що дві третини опитаних фахівців з кібербезпеки були переконані, що без штучного інтелекту неможливо вчасно та якісно реагувати на кіберінциденти.

Штучний інтелект використовується у сфері кібербезпеки для посилення захисту хмарних систем. По-перше, системи на основі штучного інтелекту можуть аналізувати великі обсяги даних, виявляти аномалії та недоліки у звичних моделях роботи, що може вказувати на спроби несанкціонованого доступу.

По-друге, штучний інтелект застосовується для розробки імунних систем, які автоматично реагують на виявлені загрози. Системи машинного навчання можуть навчитися розрізняти безпечні та потенційно небезпечні запити, забезпечуючи безперервний захист від нових кібератак.

Використання штучного інтелекту дозволяє створювати системи, які постійно вдосконалюються, адаптуються до нових загроз і вчаться на власному досвіді. Такий цикл неперервного вдосконалення забезпечує високий рівень безпеки в хмарних системах.

Отже, застосування штучного інтелекту у сфері кібербезпеки є необхідним для підвищення ефективності роботи фахівців та зниження ризику людського фактору.

Мета роботи полягає у дослідженні засад забезпечення інформаційної безпеки хмарних систем із застосуванням штучного інтелекту для захисту від кібератак.

Об'єкт дослідження – забезпечення інформаційної безпеки хмарних систем.

Предмет дослідження - особливості застосування штучного інтелекту для захисту хмарних систем від кібератак.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати основні види та особливості кібератак на хмарні системи.
2. Дослідити роль штучного інтелекту у виявленні та запобіганні кібератакам на хмарні системи.
3. Розробити рекомендації щодо впровадження штучного інтелекту для захисту хмарних систем від кібератак на основі досліджених методів та засобів.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, теорії інформаційної безпеки, теорії штучного інтелекту, а також методи машинного навчання та глибинного навчання.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту хмарних систем від кібератак, забезпечити інформаційну безпеку, підвищити стійкість інфраструктури та захистити дані підприємства відповідно до цілей бізнесу, можливостей та ресурсів підприємства.

Апробація результатів кваліфікаційної роботи було оприлюднено на

Всеукраїнської науково-практичної конференції "Стратегії кіберстійкості:управління ризиками та безперервність бізнесу"

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ХМАРНИХ СИСТЕМ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

1.1. Сутність хмарних систем та їх особливості

Хмарні системи, або хмарні обчислення, представляють собою модель надання комп'ютерних ресурсів і послуг через Інтернет. Вони включають в себе широкий спектр послуг, таких як зберігання даних, обчислювальні потужності, мережеві ресурси, програмне забезпечення та інші IT-інфраструктури, які надаються користувачам на вимогу.

Основною особливістю хмарних систем є їх здатність забезпечувати доступ до ресурсів за принципом "плати за використання", що дозволяє підприємствам і користувачам ефективно управляти витратами на IT-інфраструктуру. Користувачі можуть масштабувати використання ресурсів відповідно до їхніх потреб, збільшуючи або зменшуючи обсяги використання в будь-який момент часу.

Хмарні системи можна класифікувати за різними моделями розгортання та сервісів. Основні моделі розгортання включають:

Публічна хмара: ресурси надаються загальнодоступними провайдерами і доступні для широкого кола користувачів через Інтернет. Прикладами публічних хмарних провайдерів є Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

Приватна хмара: ресурси використовуються виключно однією організацією. Вони можуть бути розміщені як на власній інфраструктурі організації, так і на інфраструктурі третьої сторони, але при цьому доступ до них обмежений внутрішніми користувачами.

Гібридна хмара: поєднує в собі елементи як публічної, так і приватної хмари, дозволяючи переміщувати дані та додатки між ними. Це забезпечує більшу гнучкість та оптимізацію використання ресурсів.

За моделями сервісів хмарні обчислення поділяються на три основні категорії:

Інфраструктура як послуга (IaaS): надає базові обчислювальні ресурси, такі як віртуальні машини, зберігання та мережі. Користувачі можуть встановлювати операційні системи та програмне забезпечення за власним вибором. Приклади: AWS EC2, Google Compute Engine.

Платформа як послуга (PaaS): надає платформи та інструменти для розробки, тестування та розгортання додатків. Це звільняє розробників від необхідності керувати базовою інфраструктурою. Приклади: Google App Engine, Microsoft Azure App Service.

Програмне забезпечення як послуга (SaaS): надає готові до використання програми, які розміщуються та управляються хмарними провайдерами. Користувачі отримують доступ до програм через Інтернет. Приклади: Google Workspace, Microsoft Office 365.

Хмарні системи мають кілька ключових особливостей:

Масштабованість: можливість автоматично або вручну масштабувати ресурси відповідно до поточних потреб, забезпечуючи високу продуктивність та надійність.

Еластичність: здатність швидко адаптуватися до змін у навантаженні, що дозволяє оптимально використовувати ресурси.

Доступність: забезпечення високої доступності послуг та даних завдяки розподіленій архітектурі та резервуванню ресурсів.

Безпека: застосування сучасних технологій захисту даних та контролю доступу для забезпечення конфіденційності, цілісності та доступності інформації.

Економічна ефективність: зниження витрат на IT-інфраструктуру за рахунок використання моделі оплати за споживання ресурсів.

Таким чином, хмарні системи представляють собою потужний інструмент для оптимізації IT-інфраструктури підприємств, забезпечуючи високу гнучкість, масштабованість та економічну ефективність. Завдяки цим перевагам, хмарні обчислення стають дедалі популярнішими серед підприємств різного масштабу та галузей діяльності.

Хмарні системи – це модель надання IT-інфраструктури, програмного забезпечення та платформ як сервісу через Інтернет. Ця модель стає все більш популярною завдяки численним перевагам, які вона пропонує підприємствам та організаціям.

1. Гнучкість:

Хмарні системи пропонують безпрецедентний рівень гнучкості, оскільки ресурси можна масштабувати вгору або вниз залежно від потреб користувача. Це дозволяє компаніям економити кошти, коли їм не потрібні всі доступні їм ресурси, і швидко розширюватися, коли їхні потреби зростають. Це особливо корисно для компаній, які мають сезонні коливання або непередбачувані потреби в обчислювальній потужності.

2. Економічність:

Хмарні системи можуть значно знизити витрати на IT-інфраструктуру та програмне забезпечення. Це пов'язано з тим, що компаніям не потрібно купувати та обслуговувати власне обладнання та програмне забезпечення. Замість цього вони платять лише за ресурси, які вони використовують, зазвичай за підпискою. Це може призвести до значної економії коштів, особливо для малих та середніх підприємств.

3. Доступність:

Користувачі можуть отримувати доступ до хмарних ресурсів з будь-якого місця та в будь-який час, використовуючи будь-який пристрій з підключенням до Інтернету. Це робить хмарні системи ідеальними для компаній з віддаленими співробітниками або для тих, які потребують доступу до своїх даних та додатків 24/7. Це також може покращити співпрацю та продуктивність команди, оскільки співробітники можуть працювати над проектами разом, незалежно від їхнього фізичного розташування.

4. Продуктивність:

Хмарні системи можуть забезпечувати високу продуктивність та масштабованість, що робить їх ідеальними для ресурсоємних додатків. Це пов'язано з тим, що хмарні провайдери мають доступ до найсучасніших

серверних технологій та мережевих ресурсів. Це може допомогти компаніям покращити продуктивність своїх додатків та скоротити час завантаження.

5. Інновації:

Хмарні провайдери постійно інвестують у розробку нових технологій та послуг, що дає користувачам доступ до найсучасніших IT-рішень. Це може допомогти компаніям залишатися на крок попереду конкурентів та впроваджувати нові продукти та послуги швидше.

6. Інші переваги:

Окрім вищезгаданих переваг, хмарні системи також пропонують ряд інших переваг, таких як:

Простота використання: Хмарні системи зазвичай прості у використанні та налаштуванні, що робить їх доступними для компаній будь-якого розміру.

Надійність: Хмарні провайдери пропонують високий рівень надійності та гарантують доступність своїх сервісів.

Безпека: Хмарні провайдери зазвичай мають суворі заходи безпеки, які допомагають захистити дані користувачів від несанкціонованого доступу.

Однак хмарні системи також мають ряд ризиків:

Безпека: Хмарні системи можуть бути мішенню для кібератак, адже дані та ресурси зберігаються на віддалених серверах. Це робить їх вразливими до крадіжки даних, несанкціонованого доступу та інших кіберзагроз. Для пом'якшення цих ризиків важливо вибирати надійного хмарного провайдера, який має суворі заходи безпеки, та використовувати належні практики безпеки.

Відповідність: Хмарні системи повинні відповідати нормативним вимогам, які можуть бути складними та дорогими для виконання. Важливо перед вибором хмарного провайдера ретельно вивчити всі відповідні нормативні вимоги.

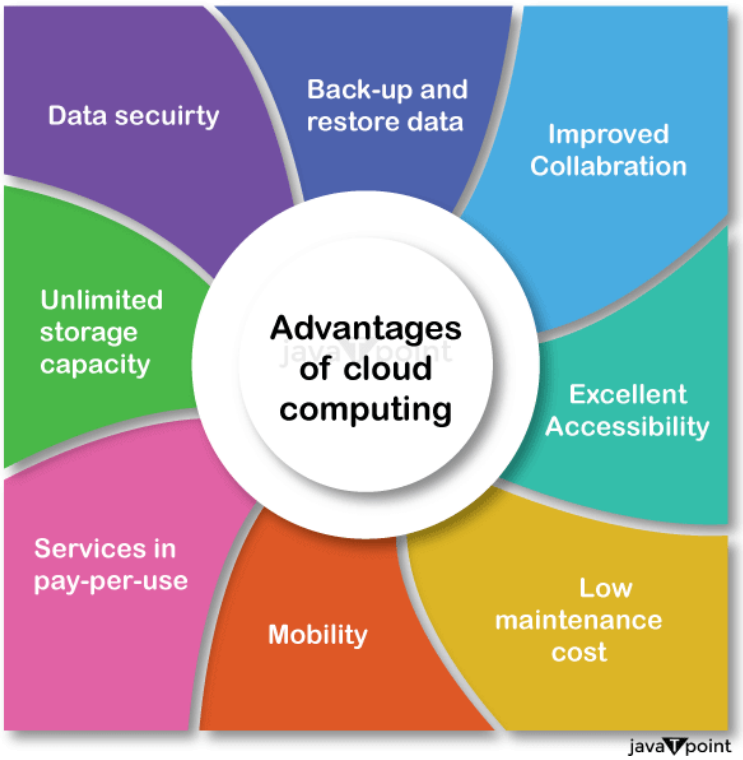

Рис. 1.1 Переваги хмарних систем

1.2. Класифікація кібератак на хмарні системи

Кібератаки на хмарні системи є серйозною загрозою, яка може призвести до значних фінансових втрат, порушення роботи та крадіжки даних. Тому важливо розуміти різні типи кібератак, які можуть бути спрямовані на хмарні системи, та вживати відповідних заходів для їх захисту.

Класифікація за типом атаки:

1. Мережеві атаки: Ці атаки спрямовані на те, щоб вивести з ладу хмарну інфраструктуру або перешкодити доступу до неї. До них належать:

- DDoS-атаки (атаки типу "відмова в обслуговуванні"): Ці атаки спрямовані на перевантаження серверів або мереж трафіком, роблячи їх недоступними для законних користувачів.
- Атаки типу "людина посередині": Ці атаки перехоплюють та маніпулюють зв'язком між двома сторонами, щоб отримати доступ до конфіденційної інформації.

- Атаки переповнення буфера: Ці атаки заповнюють буфери пам'яті комп'ютера шкідливим кодом, який може призвести до його збою або крадіжки даних.

2. Атаки на веб-додатки: Ці атаки спрямовані на те, щоб виявити та експлуатувати вразливості у веб-додатках, які розміщені в хмарі. До них належать:

- Атаки на ін'єкції SQL: Ці атаки вводять шкідливий код у SQL-запити, щоб отримати доступ до даних або виконати несанкціоновані дії.
- Міжсайтові скрипти (XSS): Ці атаки вводять шкідливий код у веб-сторінки, який може бути виконаний браузером користувача, надаючи зловмисникам доступ до його даних або комп'ютера.
- Атаки на перевірку автентичності: Ці атаки намагаються зламати механізми автентифікації веб-додатків, щоб отримати доступ до облікових записів користувачів.

3. Атаки на дані: Ці атаки спрямовані на крадіжку, викривлення або знищення даних, які зберігаються в хмарі. До них належать:

- Атаки типу "людина посередині": Ці атаки перехоплюють та маніпулюють зв'язком між двома сторонами, щоб отримати доступ до конфіденційної інформації.
- Атаки з викраденням облікових записів: Ці атаки намагаються отримати доступ до облікових записів користувачів, щоб вкрасти їхні дані або отримати доступ до хмарних ресурсів.
- Атаки з вилученням даних: Ці атаки намагаються викрасти дані з хмарних систем, наприклад, шляхом завантаження або копіювання їх.

4. Атаки на віртуальні машини: Ці атаки спрямовані на віртуальні машини, які розміщені в хмарі. До них належать:

- Атаки типу "людина посередині": Ці атаки перехоплюють та маніпулюють зв'язком між віртуальними машинами, щоб отримати доступ до конфіденційної інформації.

- Атаки з викраденням облікових записів: Ці атаки намагаються отримати доступ до облікових записів користувачів, щоб отримати доступ до віртуальних машин.
- Атаки типу "відмова в обслуговуванні": Ці атаки намагаються вивести з ладу віртуальні машини, перевантажуючи їх трафіком.

Класифікація за ціллю атаки:

- Інфраструктура: Ці атаки спрямовані на те, щоб вивести з ладу хмарну інфраструктуру, що може призвести до перебоїв у роботі та втрати даних.
- Дані: Ці атаки спрямовані на крадіжку або викривлення інформації.

1.3. Методи та інструменти захисту хмарних систем

Рис. 1.2 Методи захисту хмарних систем

Зважаючи на зростаючу загрозу кібератак, захист хмарних систем став критично важливим завданням для будь-якої організації, яка використовує хмарні послуги. Існує ряд методів та інструментів, які можна використовувати для захисту хмарних систем, які можна узагальнити наступним чином:

Фізична безпека:

- Захист центрів обробки даних: Це включає в себе контроль доступу, відеоспостереження та інші фізичні заходи безпеки, щоб запобігти несанкціонованому доступу до центрів обробки даних, де зберігаються хмарні дані та ресурси.
- Захист мережевої інфраструктури: Це включає в себе брандмауери, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) для захисту хмарної інфраструктури від мережевих атак.

Мережева безпека:

- Віртуальні локальні мережі (VLAN): VLAN дозволяють сегментувати хмарну мережу на логічні підмережі, що може допомогти обмежити поширення кібератак.
- Захист IP-адрес: Захист IP-адрес хмарних ресурсів від сканування та атак може бути досягнутий за допомогою таких методів, як списки доступу та брандмауери.
- Шифрування мережевого трафіку: Шифрування трафіку між хмарними ресурсами та користувачами може допомогти захистити дані від перехоплення та несанкціонованого доступу.

Безпека веб-додатків:

- Сканування вразливостей: Регулярне сканування веб-додатків на наявність вразливостей може допомогти виявити та виправити потенційні проблеми безпеки до того, як ними скористаються зловмисники.
- Веб-браузери: Використання оновлених веб-браузерів та налаштування безпечних налаштувань може допомогти захистити користувачів від кібератак під час доступу до хмарних веб-додатків.
- Веб-сервери: Налаштування веб-серверів з урахуванням найкращих практик безпеки може допомогти запобігти поширенню кібератак.

Шифрування:

- Шифрування даних: Шифрування даних як у стані спокою, так і під час передачі, може допомогти захистити їх від несанкціонованого доступу.

- Шифрування ключів шифрування: Шифрування ключів шифрування за допомогою методів, таких як управління ключами шифрування (KMS), може допомогти забезпечити їх безпеку.

Контроль доступу:

- Аутентифікація та авторизація: Використання надійних методів аутентифікації та авторизації для надання користувачам доступу до хмарних ресурсів може допомогти запобігти несанкціонованому доступу.
- Управління обліковими записами: Регулярний перегляд та оновлення облікових записів користувачів може допомогти забезпечити те, що лише авторизовані користувачі мають доступ до хмарних ресурсів.
- Принцип найменших привілеїв: Надання користувачам лише тих прав доступу, які їм необхідні для виконання своїх завдань, може допомогти обмежити потенційний вплив кібератаки.

Моніторинг:

- Моніторинг журналів: Моніторинг журналів активності хмарних систем може допомогти виявити ознаки кібератаки.
- Моніторинг мережевого трафіку: Моніторинг мережевого трафіку на наявність підозрілої активності може допомогти виявити кібератаки на ранній стадії.
- Моніторинг системної продуктивності: Моніторинг системної продуктивності може допомогти виявити аномалії, які можуть бути ознакою кібератаки.

1.4. Аналіз літератури та останніх дослідженнь

Використання штучного інтелекту (ШІ) в кібербезпеці привертає значну увагу дослідників по всьому світу. У цьому розділі розглянуто кілька провідних науковців, які зробили вагомий внесок у розвиток цієї галузі, а також результати їх досліджень.

Вивчення літератури та останніх досліджень у сфері забезпечення безпеки хмарних систем є критично важливим для розуміння поточних тенденцій, технологій та методів, що використовуються для захисту даних та інфраструктури. Цей розділ охоплює аналіз ключових джерел та наукових робіт, які розглядають аспекти безпеки хмарних обчислень, а також визначає напрями подальших досліджень у цій галузі.

Останні дослідження зосереджені на покращенні методів аутентифікації та авторизації для хмарних систем. Зокрема, розглядаються адаптивні методи аутентифікації, що використовують машинне навчання для аналізу поведінки користувачів та виявлення аномалій. У роботі [1] запропоновано використання поведінкової біометрії для підвищення надійності аутентифікації.

Багато досліджень присвячено розробці нових методів шифрування, що забезпечують високу продуктивність та безпеку даних у хмарних системах. Наприклад, у статті [2] представлено метод гомоморфного шифрування, який дозволяє виконувати обчислення над зашифрованими даними без необхідності їх розшифровки, що значно підвищує рівень конфіденційності.

Дослідження у цій сфері зосереджені на виявленні та запобіганні мережевим атакам, таким як DDoS-атаки. У роботі [3] запропоновано метод використання машинного навчання для аналізу мережевого трафіку та виявлення аномалій, що свідчать про DDoS-атаки.

Останні дослідження також охоплюють питання безпеки веб-додатків у хмарних системах. Наприклад, у статті [4] запропоновано використання веб-фаєрволів (WAF) у поєднанні з машинним навчанням для автоматичного виявлення та блокування атак на веб-додатки.

Використання штучного інтелекту та машинного навчання для забезпечення безпеки хмарних систем є однією з провідних тенденцій у цій галузі. У роботі [5] розглянуто використання глибокого навчання для прогнозування кіберзагроз та автоматизації процесів реагування на інциденти.

1.4.1 Дослідники

Хіндрі Адріан Сантоса є провідним дослідником у галузі машинного навчання та штучного інтелекту, зосереджуючись на виявленні кіберзагроз. Його дослідження спрямовані на розробку та вдосконалення моделей глибокого навчання для автоматичного виявлення аномалій у мережевому трафіку.

Сантоса активно працює з рекурентними нейронними мережами (RNN), які виявилися надзвичайно ефективними для аналізу послідовних даних. Ці мережі дозволяють виявляти відхилення від звичайних патернів трафіку, що може свідчити про можливі кібератаки. Його дослідження показали, що використання RNN значно підвищує точність та швидкість виявлення аномалій порівняно з традиційними методами, такими як методи на основі правил або статистичного аналізу.

Одним із ключових аспектів роботи Сантоси є тестування розроблених моделей на реальних даних, зібраних з мережевих систем, що включає співпрацю з промисловими партнерами. Цей підхід допомагає впроваджувати розроблені методи в практичні системи кібербезпеки, забезпечуючи високу ефективність виявлення та запобігання кібератакам.

Еліза Бертіно є провідним дослідником у галузі інформаційної безпеки та захисту даних, зокрема у сфері хмарних обчислень. Вона працює над розробкою методів, що забезпечують безпеку і конфіденційність даних у хмарних середовищах. Основним напрямком її досліджень є використання політик доступу та управління ідентифікацією для захисту конфіденційних даних.

Бертіно зосереджується на створенні механізмів, які дозволяють забезпечити безпеку даних у хмарі без необхідності довіряти повністю хмарному провайдеру. Її дослідження включають розробку криптографічних методів для захисту даних під час їх обробки в хмарі, таких як шифрування з можливістю виконання пошукових запитів та обчислень над зашифрованими даними. Це дозволяє користувачам зберігати та обробляти свої дані в хмарі, зберігаючи при цьому конфіденційність.

Однією з ключових тем досліджень Бертіно є розробка моделей політик доступу, що дозволяють динамічно змінювати права доступу до даних залежно від контексту, наприклад, місцезнаходження користувача або часу доби. Це значно підвищує гнучкість та безпеку систем захисту даних у хмарних середовищах. Результати її досліджень сприяють розвитку інноваційних підходів до захисту даних, забезпечуючи більш високий рівень безпеки та конфіденційності для користувачів хмарних сервісів.

Джонні Іваноскі - провідний дослідник у галузі кібербезпеки, зокрема у сфері аналізу та виявлення загроз за допомогою сучасних технологій. Його дослідження зосереджені на розробці передових методів для виявлення та запобігання кібератакам, а також на застосуванні машинного навчання та штучного інтелекту для підвищення ефективності систем кіберзахисту.

Іваноскі активно працює над створенням алгоритмів машинного навчання, здатних аналізувати великі обсяги даних і виявляти аномалії, що можуть свідчити про кібератаки. Він досліджує, як різні моделі машинного навчання, включаючи глибокі нейронні мережі, можуть бути використані для аналізу поведінкових патернів у мережевому трафіку. Його робота показала, що застосування таких технологій дозволяє значно підвищити точність виявлення загроз порівняно з традиційними методами.

Однією з ключових цілей досліджень Іваноскі є інтеграція розроблених методів у реальні системи кібербезпеки. Він працює над проектами, які включають тестування алгоритмів на реальних даних та співпрацю з індустріальними партнерами для впровадження цих рішень у практичні системи захисту. Його дослідження сприяють розвитку нових підходів до кібербезпеки, що забезпечують вищий рівень захисту мережевих систем та даних.

Лізхен Ян є провідним дослідником у галузі кібербезпеки та захисту даних, зокрема у сфері безпеки хмарних обчислень та великих даних. Вона працює над розробкою методів забезпечення конфіденційності та цілісності даних у хмарних середовищах, а також над удосконаленням механізмів виявлення кіберзагроз.

Одним із основних напрямків досліджень Ян є використання алгоритмів машинного навчання для виявлення аномалій у великих обсягах даних. Вона розробляє моделі, які можуть автоматично аналізувати поведінку користувачів та систем, виявляючи потенційні загрози та порушення безпеки. Її робота зосереджена на створенні алгоритмів, здатних виявляти не лише відомі, але й нові, невідомі загрози, що робить системи кібербезпеки більш адаптивними та ефективними.

Ян також активно досліджує питання захисту конфіденційних даних під час їх обробки та передачі у хмарних середовищах. Вона працює над розробкою криптографічних методів, що дозволяють зберігати та обробляти дані, зберігаючи при цьому їхню конфіденційність. Її дослідження сприяють розвитку інноваційних технологій захисту даних, забезпечуючи більш високий рівень безпеки для користувачів хмарних сервісів.

Висновоки до розділу 1

Хмарні системи пропонують безліч переваг для організацій, таких як гнучкість, економічність, доступність та інновації. Однак вони також схильні до різних кіберзагроз, які можуть призвести до значних фінансових втрат, порушення роботи та крадіжки даних.

Захист хмарних систем є критично важливим завданням, і для цього можна використовувати ряд методів та інструментів. Ці методи включають фізичну безпеку, мережеву безпеку, безпеку веб-додатків, шифрування, контроль доступу та моніторинг.

Штучний інтелект (ШІ) може відігравати значну роль у посиленні захисту хмарних систем. ШІ-системи здатні виявляти аномалії, аналізувати журнали та автоматизувати реагування на інциденти, що може допомогти організаціям швидше та ефективніше виявляти та реагувати на кібератаки.

Наступні розділи цього дослідження будуть присвячені детальному вивченню методів та алгоритмів на основі ШІ для захисту хмарних систем.

Дослідники розроблять нові підходи, оцінять їх ефективність у експериментах та сформулюють практичні рекомендації для організацій, які хочуть використовувати ШІ для покращення кібербезпеки своїх хмарних систем.

Очікується, що результати цього дослідження допоможуть удосконалити захист хмарних систем і зробити їх більш стійкими до кіберзагроз.

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ХМАРНИХ СИСТЕМ НА ОСНОВІ ШІ

2.1. Огляд існуючих методів та алгоритмів

Останні роки свідчать про значний прогрес у дослідженнях, присвячених використанню штучного інтелекту для захисту хмарних систем. Цей напрям розвитку в кібербезпеці приніс широкий спектр інструментів та алгоритмів, які використовуються для вирішення різноманітних завдань забезпечення безпеки. Результатом цих досліджень є розробка передових методів, що надійно захищають хмарні інфраструктури від потенційних загроз. Серед них можна виділити алгоритми машинного навчання, які використовуються для виявлення аномалій та прогнозування кібератак, а також системи ідентифікації та аутентифікації, що використовують біометричні дані та інші методи для забезпечення безпеки доступу до хмарних ресурсів.

Цей широкий спектр інноваційних методів і технологій відкриває нові можливості для ефективного захисту хмарних систем від різноманітних загроз. Завдяки використанню штучного інтелекту та машинного навчання, розробники отримують можливість створювати адаптивні системи, які навчаються і вдосконалюються з часом, що дозволяє їм ефективно протистояти навіть найбільш складним атакам.

Ці інноваційні підходи в області кібербезпеки стають важливим інструментом для сучасних організацій, які прагнуть забезпечити безпеку своїх даних та інфраструктури в хмарних середовищах. Впровадження передових методів захисту на основі штучного інтелекту є ключовим кроком у напрямку забезпечення стійкості та надійності хмарних сервісів у сучасному цифровому світі.

2.1.1. Приклади існуючого інструментарію

Для забезпечення безпеки хмарних систем існує широкий спектр інструментів та платформ, які реалізують різноманітні методи та алгоритми захисту. Нижче наведені приклади основних інструментів, що застосовуються для аутентифікації та авторизації, шифрування, мережевого захисту та захисту від DDoS-атак.

Auth0 - це платформа аутентифікації та авторизації як послуга (AAaaS), що дозволяє розробникам легко інтегрувати функції аутентифікації та авторизації в свої додатки. Забезпечує безпечний доступ до додатків, API та пристроїв, використовуючи сучасні методи аутентифікації. Ключові функції включають підтримку різних методів входу, ролі та дозволи для контролю доступу, багатофакторну аутентифікацію та управління користувачами.

Auth0 дозволяє розробникам легко додавати захищений доступ до своїх додатків та сервісів через різні методи аутентифікації, включаючи соціальні мережі та багатофакторну аутентифікацію. Крім того, можливість налаштування ролей та дозволів дозволяє контролювати доступ до різних частин додатка на основі ролі користувача.

Auth0 також надає інструменти для управління користувачами, включаючи створення та оновлення профілів, налаштування автентифікаційних правил та моніторинг активності. Це допомагає адміністраторам тримати контроль над безпекою та активністю користувачів. Auth0 підтримує широкий спектр платформ та мов програмування, що забезпечує високу гнучкість та масштабованість для розробників. Детальніше про можливості Auth0 можна дізнатися [6].

Okta - це ще одна платформа аутентифікації та авторизації як послуга (AAaaS), яка дозволяє розробникам легко інтегрувати функції аутентифікації та авторизації в свої додатки. Платформа надає широкі можливості для безпечного доступу до додатків, API та пристроїв, використовуючи сучасні методи

аутентифікації. Однією з ключових функцій Okta є підтримка різних методів входу, таких як соціальні мережі, багатофакторна аутентифікація та інші.

У порівнянні з Auth0, Okta також пропонує рішення для управління користувачами та контролю доступу, включаючи налаштування ролей та дозволів. Це дозволяє розробникам ефективно керувати доступом до різних частин своїх додатків на основі ролей та прав доступу користувачів.

Додатково, Okta надає інтеграцію з різноманітними іншими сервісами та інструментами, що робить його популярним вибором для комплексних проектів. Це забезпечує розробникам гнучкість та можливість інтегрувати Okta з різними технологічними стеками.

Для отримання більш детальної інформації про можливості та функціонал Okta, рекомендується ознайомитися з офіційною документацією[7].

Azure Active Directory (AAD) - це послуга ідентифікації в хмарі від Microsoft, яка надає засоби для управління ідентичністю та доступом до ресурсів в хмарних та локальних середовищах. AAD дозволяє компаніям керувати користувачами, групами та додатками, надаючи безпечний доступ до різних сервісів та додатків.

Однією з ключових можливостей Azure Active Directory є єдина ідентичність для автентифікації користувачів у різних хмарних та локальних середовищах. Це дозволяє користувачам використовувати одні й ті ж облікові записи для входу в різні додатки та сервіси, спрощуючи управління ідентичністю.

Крім того, Azure Active Directory забезпечує різноманітні засоби для захисту доступу, включаючи багатофакторну аутентифікацію, управління правами доступу та моніторинг активності користувачів. Це дозволяє компаніям підвищити безпеку своїх ресурсів та даних.

Шифрування - це процес захисту даних шляхом перетворення їх у незрозумілу форму за допомогою математичних алгоритмів. Це забезпечує конфіденційність інформації, оскільки навіть якщо дані стануть доступні незаконним особам, без спеціального ключа їх важко або навіть неможливо

розшифрувати. Шифрування використовується для захисту даних під час їх передачі через мережі, зберігання на серверах або в облаках, а також на пристроях користувачів, таких як смартфони і комп'ютери. Цей процес включає в себе використання ключів, які визначаються алгоритмом шифрування і використовуються для зашифрування та розшифрування даних.

Amazon Web Services Key Management Service (AWS KMS) - це керований сервіс для створення та керування ключами шифрування у хмарному середовищі AWS. Він надає можливість легко створювати та керувати ключами шифрування для захисту даних в AWS. AWS KMS дозволяє створювати та керувати ключами шифрування, які використовуються для шифрування та розшифрування даних у різних сервісах та додатках AWS.

Однією з ключових можливостей AWS KMS є можливість інтеграції з іншими сервісами AWS, такими як Amazon S3, Amazon EBS та Amazon Redshift. Це дозволяє автоматично зашифровувати дані, що зберігаються в цих сервісах, забезпечуючи високий рівень безпеки даних. Крім того, AWS KMS надає можливість керувати доступом до ключів шифрування та виконувати аудит дій з ними для забезпечення відповідності вимогам безпеки.

AWS KMS також підтримує різні типи ключів шифрування, включаючи симетричні та асиметричні ключі. Це дозволяє користувачам вибирати найбільш підходящий тип ключа для їх конкретних потреб безпеки даних. Крім того, AWS KMS надає можливість інтеграції зі сторонніми сервісами та додатками через різноманітні API, що робить його високоякісним рішенням для захисту конфіденційної інформації в хмарному середовищі AWS.

Опис: KMS – це керована служба шифрування від Amazon Web Services, яка дозволяє легко створювати і контролювати ключі шифрування.

Особливості: Інтеграція з іншими сервісами AWS, підтримка як симетричного, так і асиметричного шифрування, аудит доступу до ключів.

Google Cloud Key Management Service (Cloud KMS)

Опис: Cloud KMS – це служба від Google Cloud для управління криптографічними ключами, що використовується для шифрування даних у хмарі.

Особливості: Інтеграція з іншими сервісами Google Cloud, підтримка гібридних ключів, автоматизація процесів управління ключами.

HashiCorp Vault

Опис: Vault – це інструмент для управління секретами та захисту конфіденційних даних шляхом шифрування.

Особливості: Підтримка динамічних секретів, управління сертифікатами та ключами, інтеграція з різними системами аутентифікації.

Мережевий захист

AWS Shield

Опис: AWS Shield – це керована служба захисту від DDoS-атак для ресурсів Amazon Web Services.

Особливості: Захист на рівні мережі та додатків, автоматичне виявлення та мітигація атак, інтеграція з іншими сервісами AWS.

Cloudflare

Опис: Cloudflare – це мережевий сервіс, що надає CDN, захист від DDoS-атак, веб-фаєрвол (WAF) та інші засоби мережевої безпеки.

Особливості: Глобальна мережа серверів для розподілу навантаження, ефективний захист від DDoS, інтеграція з багатьма веб-платформами.

Cisco Umbrella

Опис: Cisco Umbrella – це хмарний сервіс безпеки, що забезпечує захист від шкідливих веб-сайтів, фішинг-атак та інших кіберзагроз.

Особливості: DNS-безпека, захист від шкідливих програм, моніторинг та аналіз трафіку.

Захист від DDoS-атак

Akamai Kona Site Defender

Опис: Kona Site Defender – це рішення від Akamai для захисту веб-додатків від DDoS-атак та інших кіберзагроз.

Особливості: Високопродуктивний захист, інтеграція з CDN, автоматичне виявлення та блокування атак.

Imperva Incapsula

Опис: Incapsula – це хмарний сервіс захисту веб-додатків, що надає захист від DDoS-атак, WAF та CDN.

Особливості: Комплексний захист веб-додатків, висока ефективність виявлення та мітигації атак, інтеграція з іншими сервісами безпеки.

Radware DefensePro

Опис: DefensePro – це рішення для захисту від DDoS-атак та інших мережевих загроз, що використовує поведінковий аналіз для виявлення аномалій.

Особливості: Захист на рівні мережі та додатків, виявлення та мітигація в режимі реального часу, інтеграція з іншими продуктами Radware.

•Scikit-learn: Ця бібліотека Python пропонує широкий спектр алгоритмів машинного навчання, які можна використовувати для виявлення аномалій, класифікації кібератак, прогнозування ризиків та інших задач.

Рис. 2.1 Логотип Scikit learn

•TensorFlow: Ця платформа з відкритим кодом використовується для розробки та розгортання моделей глибокого навчання. Її можна використовувати для виявлення аномалій, аналізу даних журналів та інших задач.

Рис. 2.2 Логотип TensorFlow

•Microsoft Azure Machine Learning: Ця платформа хмарних обчислень пропонує широкий спектр інструментів для машинного навчання, які можна використовувати для захисту хмарних систем.

Рис. 2.3 Логотип Microsoft Azure Machine Learning

•IBM Watson for Cybersecurity: Ця платформа використовує ШІ для автоматизації аналітики кібербезпеки та реагування на інциденти.

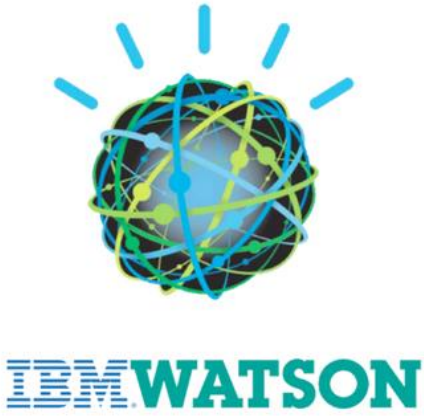

Рис. 2.4 Логотип IBM Watson for Cybersecurity

2.1.2. Вибір інструментарію

Вибір інструментарію для захисту хмарних систем на основі ШІ залежить від конкретних потреб та задач.

У цьому дослідженні ми будемо використовувати бібліотеку Scikit-learn як приклад.

Scikit-learn (скорочено sklearn) – це безкоштовна та відкрита бібліотека машинного навчання для мови програмування Python. Вона пропонує широкий набір інструментів і алгоритмів для виконання різноманітних завдань машинного навчання, зокрема: класифікація, регресія, кластеризація, обробка даних, оцінювання моделі.

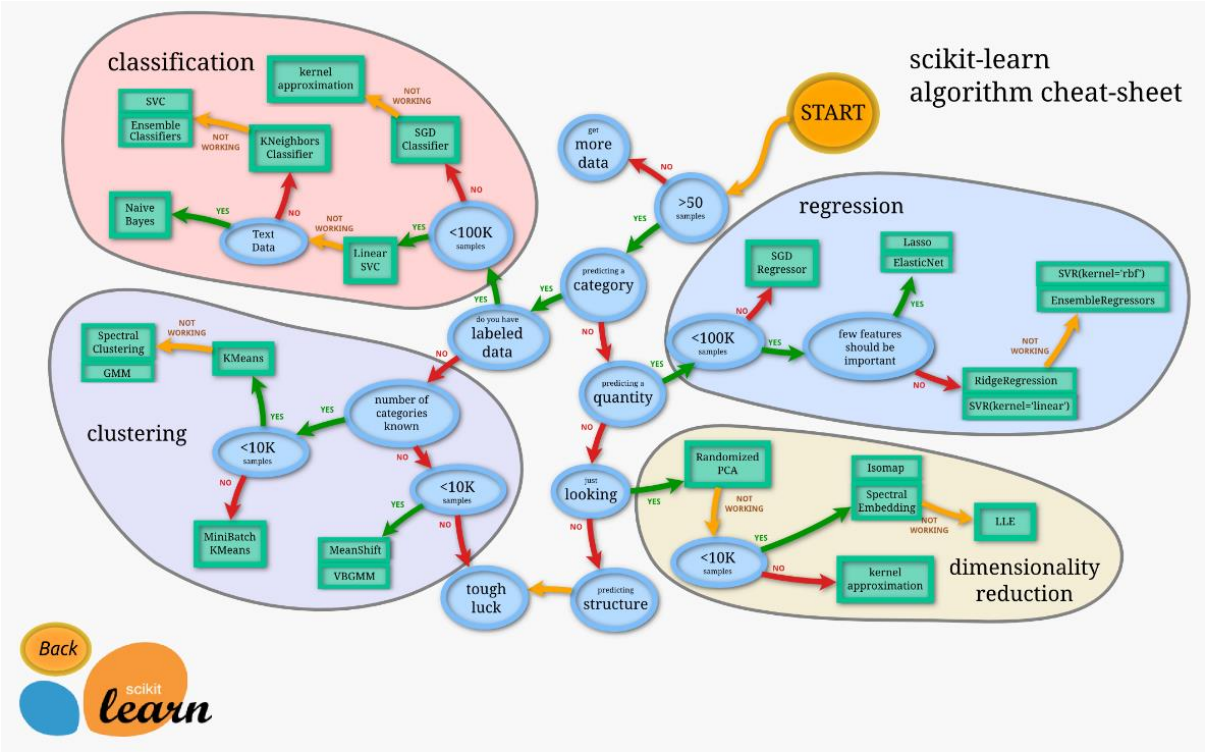

Рис. 2.5 Підказка для вибору правильного алгоритму

2.1.3. Практичний приклад з Scikit-learn

Для виявлення аномалій в хмарній системі можна використовувати алгоритм Local Outlier Factor (LOF) з бібліотеки Scikit-learn.

Цей алгоритм виявляє точки даних, які значно відрізняються від своїх сусідів.

Наприклад, LOF може бути використаний для виявлення незвичайних сплесків трафіку або підозрілої активності користувачів.

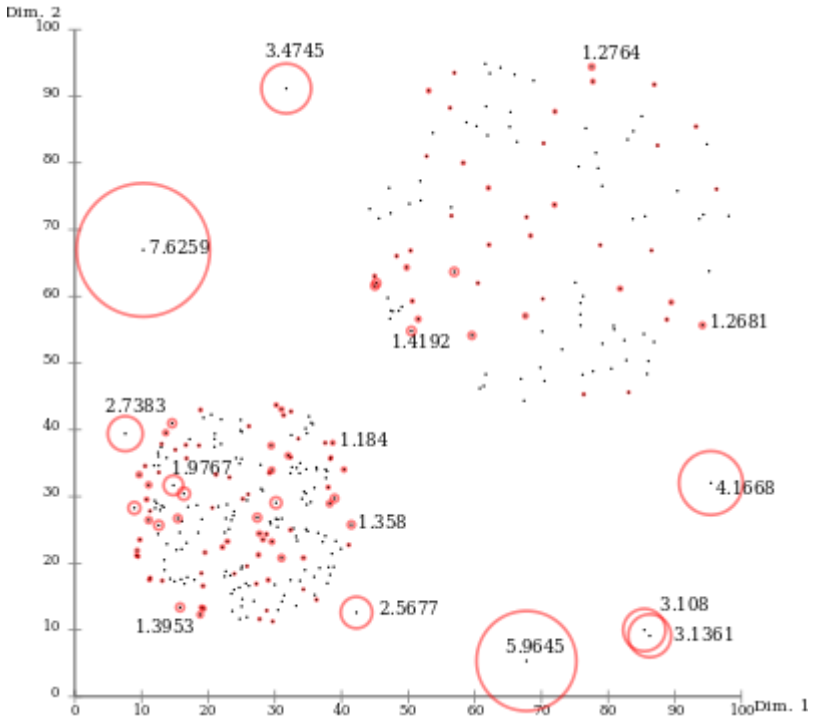

Рис. 2.6 Результати роботи алгоритму Local Outlier Factor (LOF) для виявлення аномалій у даних.

Крапки на діаграмі(Рис. 2.6) представляють дані, які були проаналізовані алгоритмом LOF. Червоні круги різного розміру позначають міру локального коефіцієнта аномальності (LOF) для кожної точки. Чим більший круг, тим більша ймовірність того, що ця точка є аномалією. Кластеризовані області з меншими колами представляють точки з низьким коефіцієнтом LOF, тобто такі, що знаходяться в областях високої щільності даних і вважаються нормальними. Одиничні точки або невеликі групи точок з великими колами вказують на точки з високим коефіцієнтом LOF, які можуть бути потенційними аномаліями.

Діаграма чітко показує, що алгоритм LOF успішно ідентифікує аномалії серед нормальних даних. Великі червоні круги вказують на аномальні точки, які мають значно нижчу щільність сусідів, в той час як менші круги представляють нормальні дані в густонаселених областях. Цей підхід є ефективним для виявлення локальних аномалій, що є особливо корисним в задачах кібербезпеки, таких як виявлення незвичайної мережевої активності або підозрілих транзакцій.

2.2. Використання алгоритму Local Outlier Factor (LOF) для виявлення аномалій

2.2.1. Опис алгоритму LOF

LOF (Local Outlier Factor) – це алгоритм машинного навчання, який використовується для виявлення аномальних даних. Він ґрунтується на ідеї, що аномальні точки даних значно відрізняються від своїх сусідів.

LOF працює наступним чином:

1) Розрахунок відстані: Для кожної точки даних алгоритм LOF розраховує відстань до її k найближчих сусідів.

2) Визначення локальної щільності: Локальна щільність точки даних визначається як обернена сума відстаней до її k найближчих сусідів.

3) Визначення фактора локального викиду: Фактор локального викиду (LOF) точки даних визначається як співвідношення локальної щільності даної точки до локальної щільності її k найближчих сусідів.

4) Виявлення аномалій: Точки даних з високим значенням LOF (більше 1) вважаються аномальними.

2.2.2. Застосування LOF для виявлення аномалій в хмарних системах

LOF може бути використаний для виявлення аномалій в хмарних системах, таких як:

- Незвичайні сплески трафіку: LOF може виявити незвичайні сплески трафіку, які можуть бути ознакою DDoS-атаки або іншої кібератаки.
- Підозріла активність користувачів: LOF може виявити підозрілу активність користувачів, таку як несанкціонований доступ до даних або незвичайні дії в системі.
- Аномалії в журналах: LOF може виявити аномалії в журналах системи, які можуть бути ознакою кібератаки або іншої несправності.

2.2.3. Приклад використання LOF

Уявімо, що нам потрібно виявити аномальні сплески трафіку в хмарній системі.

Першим кроком буде збір даних про трафік. Ці дані можуть включати в себе час, IP-адресу джерела, IP-адресу призначення, порт джерела, порт призначення та обсяг даних.

Після збору даних ми можемо використовувати алгоритм LOF для обчислення фактора локального викиду для кожної точки даних.

Процес складається з наступних кроків:

1) Вибір параметра k: Визначається кількість найближчих сусідів (зазвичай квадратний корінь з кількості точок даних).

2) Розрахунок відстані: Використовується евклідова або манхеттенська відстань до k найближчих сусідів для кожної точки.

3) Визначення локальної щільності: Розраховується як обернена сума відстаней до k найближчих сусідів: Локальна щільність = 1 / Σd_i де d_i - відстань до i-го найближчого сусіда.

4) Визначення LOF: Визначається як співвідношення локальної щільності точки до локальної щільності її k найближчих сусідів: LOF = (Локальна щільність точки) / (Середня локальна щільність k найближчих сусідів)

5) Виявлення аномалій: Точки з LOF більше 1 вважаються аномальними.

LOF візуалізується графіком, де аномальні точки розташовані далеко від інших.

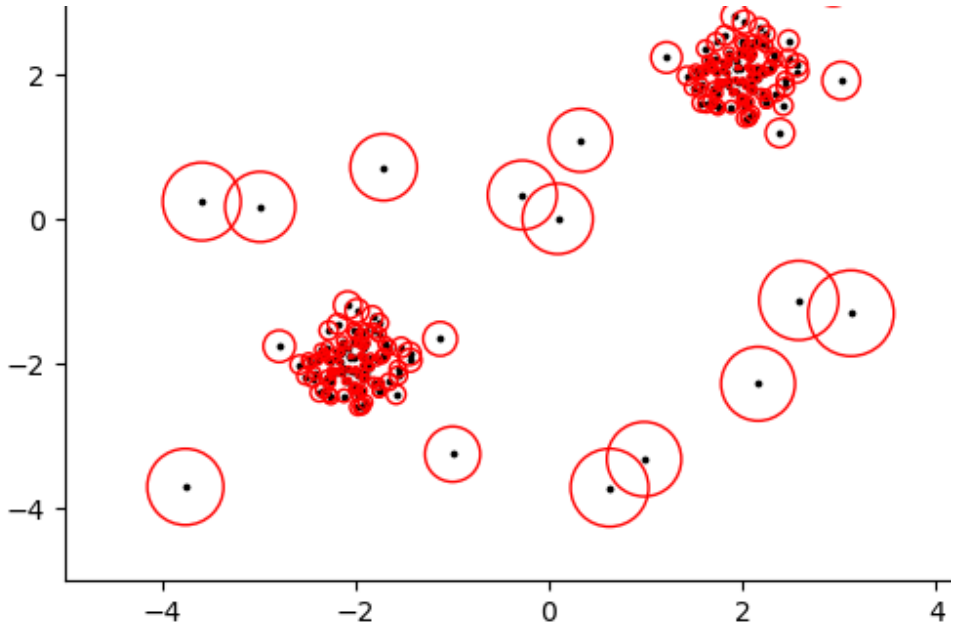

Рис. 2.7 Ще один приклад результату роботи алгоритму LOF

Інтерпретація результатів вимагає додаткового розслідування, щоб визначити причину аномальних даних.

Приклад:

Уявімо, що у нас є набір даних про трафік, що містить 1000 точок даних.

Ми вибираємо значення k = 10 і використовуємо алгоритм LOF для обчислення LOF для кожної точки даних, візуалізуємо результати LOF за допомогою графіка, в результаті чого виявляємо, що 10 точок даних мають високе значення LOF. Після цього ми досліджуємо ці 10 точок даних і виявляємо, що вони всі походять з однієї IP-адреси. Це може бути ознакою DDoS-атаки з цієї IP-адреси.

LOF – це лише один з багатьох алгоритмів, які можуть бути використані для захисту хмарних систем на основі ШІ.

2.3. Переваги та недоліки алгоритму LOF

2.3.1. Переваги:

•Ефективність: LOF може швидко обробляти великі набори даних.

•Гнучкість: LOF не залежить від припущень про розподіл даних.

•Розуміння контексту: LOF враховує локальну щільність даних, що робить його більш стійким до шуму та аномалій.

•Інтерпретованість: LOF генерує значення фактора LOF для кожної точки даних, яке можна використовувати для ранжирування потенційних викидів.

2.3.2. Недоліки:

•Чутливість до шуму: LOF може бути чутливим до шуму в даних, що може призвести до помилкового визначення викидів.

•Залежність від масштабу: LOF чутливий до масштабу даних, тому його необхідно нормалізувати перед застосуванням.

•Висока обчислювальна складність: LOF може бути обчислювально складним для великих наборів даних.

•Необхідність визначення параметрів: LOF потребує визначення параметра minPts, який впливає на визначення локальної щільності.

2.4. Застосування алгоритму LOF в хмарних системах

У цьому тексті ми розглянули лише один із прикладів застосування алгоритму LOF – його використання в хмарних системах.

Насправді, LOF має значно ширший спектр застосування. Його можна використовувати в різних сферах, таких як:

•Фінанси: Виявлення шахрайства, відмивання грошей, незвичайних транзакцій.

•Охорона здоров'я: Виявлення аномальних результатів аналізів, помилок у діагностиці, незвичайних медичних випадків.

•Виробництво: Виявлення аномальних показників роботи обладнання, дефектів продукції, несправностей в системі.

•Маркетинг: Виявлення аномальних патернів поведінки клієнтів, шахрайства в рекламних кампаніях, неефективних маркетингових стратегій.

Завдяки своїй універсальності, простоті та ефективності, LOF є цінним інструментом для аналізу даних, який може допомогти у вирішенні багатьох задач.

Висновоки до розділу 2

У цьому розділі ми детально розглянули алгоритм LOF (Local Outlier Factor).

Ми вивчили його основні принципи роботи, етапи алгоритму, переваги та недоліки, а також його інтерпретацію та візуалізацію.

LOF – це алгоритм, який використовується для виявлення аномальних даних в різних наборах даних.

Він простий у реалізації та розумінні, не потребує маркованих даних для навчання і може бути дуже ефективним у виявленні аномальних даних.

Однак LOF може бути чутливим до вибору параметра k і може мати труднощі з виявленням аномальних даних, які знаходяться в щільних кластерах з нормальними даними.

Важливо розуміти переваги та недоліки алгоритму LOF для того, щоб використовувати його ефективно в різних задачах.

РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ХМАРНИХ СИСТЕМ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

3.1. Аналіз існуючих методів захисту хмарних систем

Забезпечення безпеки хмарних систем є критично важливим завданням для будь-якої організації, яка використовує або планує використовувати хмарні обчислення. Існуючі методи захисту хмарних систем охоплюють широкий спектр технологій і практик, спрямованих на захист даних, інфраструктури та користувачів від різноманітних загроз. У цьому розділі розглядаються основні методи та підходи до забезпечення безпеки хмарних систем.

Одним з ключових аспектів захисту хмарних систем є забезпечення надійної аутентифікації та авторизації користувачів. Це важливо для того, щоб переконатися, що лише вповноважені особи мають доступ до системних ресурсів і дані залишаються безпечними. Сучасні методи включають:

Многофакторну аутентифікацію (MFA): Цей метод використовує декілька факторів для підтвердження особи користувача. Вони можуть включати пароль, одноразовий код, біометричні дані та інші. Застосування декількох факторів значно знижує ризик несанкціонованого доступу, оскільки навіть якщо один з факторів стане компромісним, інші залишаються надійними.

Рольову модель доступу (RBAC): Цей метод передбачає надання доступу до ресурсів на основі ролей користувачів. Користувачам надаються відповідні ролі з відповідними привілеями, що обмежує їхній доступ тільки до необхідних ресурсів для виконання їх робочих обов'язків. Це дозволяє ефективно обмежувати доступ до критично важливих ресурсів і запобігати несанкціонованому використанню.

Управління ідентифікацією та доступом (IAM): Цей підхід передбачає використання систем IAM для централізованого управління обліковими записами користувачів та контролю доступу до ресурсів хмарної системи. IAM дозволяє адміністраторам ефективно управляти правами доступу користувачів, встановлюючи політики доступу, перевіряючи безпеку паролів та моніторячи

активність користувачів для виявлення можливих загроз.На сьогодні існують різноманітні методи захисту хмарних систем, які можна умовно розділити на три категорії, кожна з яких має свої переваги та обмеження.

Перша категорія - це традиційні методи захисту, які включають у себе фаєрволи, системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), а також антивірусне програмне забезпечення. Ці методи широко використовуються для захисту мереж і комп'ютерів вже протягом багатьох років і добре справляються з відомими загрозами. Проте, вони не завжди ефективні у боротьбі з новими та складними атаками, оскільки їхні правила та сигнатури можуть бути неактуальними для нових загроз.

Друга категорія - це методи, що базуються на хмарних технологіях, такі як віртуальні приватні мережі (VPN), шифрування даних та контроль доступу на основі ролей (RBAC). Ці методи дозволяють забезпечити додатковий рівень захисту для хмарних інфраструктур, особливо у випадках, коли дані передаються через непридатні для довіри мережі, такі як Інтернет. Однак, їх впровадження може бути складним та витратним, і вони можуть створювати додаткові обмеження щодо доступу до даних.

Третя категорія - це методи, що базуються на штучному інтелекті, такі як машинне навчання, аналіз аномалій та прогнозування кібератак. Ці методи є перспективними у захисті хмарних систем, оскільки вони можуть автоматизувати процес виявлення та реагування на кібератаки, а також прогнозувати та запобігати їм. Вони виявляються ефективними у виявленні навіть нових атак, які можуть бути не знані традиційним методам захисту. Однак, їх ефективність може залежати від якості та обсягу навчальних даних, а також від рівня експертизи персоналу.

3.2. Практичний приклад використання методів ШІ в кібербезпеці

Цей розділ присвячений практичному прикладу використання методів штучного інтелекту (ШІ) в роботі фахівця з кібербезпеки. Уявімо, що ви –

фахівець з кібербезпеки, який відповідає за захист хмарної інфраструктури вашої компанії. Ви використовуєте ряд методів ШІ для автоматизації та покращення вашої роботи.

3.2.1 Система виявлення аномалій

Система виявлення аномалій: система використовує алгоритми машинного навчання для аналізу поведінки користувачів та трафіку даних. Система може виявляти аномальні дії, які можуть бути ознакою кібератаки.

Така система допомагає ефективніше помічати аномальну активність, що може призвести до кіберінциденту, а також зєкономити час спеціаліста, який може займатися іншими питаннями замість постійного моніторингу за трафіком.

Як працює система виявлення аномалій на основі Splunk:

1) Збір даних: Splunk може збирати дані з різних джерел, таких як журнали безпеки, записи про мережевий трафік, дані про продуктивність та інші дані.

2) Навчання моделі: Splunk використовує алгоритми машинного навчання для навчання на основі зібраних даних. Модель навчається виявляти нормальну поведінку.

3) Виявлення аномалій: Splunk використовує навчену модель для виявлення аномальних дій. Аномальні дії можуть включати незвичайні дії користувачів, незвичайні піки трафіку даних або інші аномалії.

4) Повідомлення про аномалії: Splunk може повідомляти про аномальні дії фахівцям з кібербезпеки різними способами, наприклад, електронною поштою, SMS або через веб-інтерфейс.

Переваги використання Splunk для виявлення аномалій:

- Можливість збирати дані з різних джерел.
- Можливість використовувати алгоритми машинного навчання для виявлення аномалій.
- Можливість гнучкої настройки правил виявлення аномалій.

- Можливість візуалізації даних про аномалії.

Для початку потрібно встановити Splunk на ваш комп'ютер або сервер. Після чого підготувати дані: Переконайтеся, що дані з вашої системи (логи, метрики тощо) надходять до Splunk. Це може включати налаштування джерела даних, наприклад, файлів журналу або API. Наступний крок - створення пошукових запитів. Потрібно створити пошукові запити, щоб визначити, які дані ви хочете аналізувати. Наприклад, ви можете шукати підозрілі активності або незвичайні відхилення від звичайного. Після цього йде єтап налаштування аномалії. Можливості Splunk будуть використані для виявлення аномалій. Це може включати використання алгоритмів машинного навчання або створення власних правил для виявлення аномальних паттернів у ваших даних. Отсаннім кроком буде встановлення сповіщення, щоб отримувати повідомлення про виявлені аномалії. Це дозволить вам оперативно реагувати на потенційні проблеми або загрози. Також важливо не забувати про тестування і оптимізацію. Протестувавши свої налаштування на реальних даних, вносьте корективи, якщо потрібно, щоб забезпечити ефективне виявлення аномалій.

Рис. 3.1 Вікно встановлення Splunk

Налаштування Splunk для виявлення аномалій може бути складним процесом, але слід дотримуватися цих кроків і використовувати доступні ресурси та документацію для покращення вашого розуміння інструменту.

3.2.2 Система прогнозування кібератак

Система прогнозування кібератак: система використовує алгоритми машинного навчання для прогнозування ймовірності кібератаки. Система може ьвизначити ймовірні цілі атак та вжити превентивних заходів.

Від попереднього пункту, тобто від системи виявлення аномалій, ця система відрізняється тим, що використовується для виявлення не тільки аномалій, але й для виявлення потенційної кібератаки.

Для реалізації даної системи потрібно розробити моделі прогнозування. Використовуються дані, зібрані у Splunk, для розробки моделей машинного навчання або статистичних моделей, які можуть передбачити можливі кібератаки. При цьому враховуються різні патерни поведінки, незвичайні активності та інші фактори, які можуть вказувати на можливі загрози.

Після цього слідує тестування та валідація моделей: Перевіряється ефективність розроблених моделей на історичних даних та на реальних випадках. Необхідно переконатися, що моделі здатні точно передбачати кібератаки та мають низький рівень помилок.

Наступним кроком йде інтеграція розроблених моделей прогнозування з існуючими системами безпеки, такими як сім'ї безпеки або системи виявлення вторгнень, забезпечуючи автоматичне виявлення та реагування на передбачені загрози.

Не потрібно забувати і про постійне навчання моделей. Продовжуючи вдосконалювати ваші моделі прогнозування, враховуючи нові дані та зміни в ландшафті кібербезпеки, використовуючи для чього механізми автоматичного навчання та адаптації для підтримки актуальності моделей можна досягти найвищого рівня точності.

Останнім кроком йде моніторинг та оцінка результатів. Ні одна з систем не буде працювати так як заплановано з першого запуску, кожна система потребує подальшого вдосконалення та\або внесення додаткових корекцій.

3.2.3 Система автоматизованого реагування на кібератак

Система автоматизованого реагування на кібератаки: система використовує алгоритми машинного навчання для автоматичного реагування на кібератаки. Система може блокувати атаки, ізолювати заражені системи та відновлювати пошкоджені дані.

Ця система корисна тим, що дозволяє спеціалісту не реагувати на типові помилки дозволяючи ПЗ самому реагувати на аномалії, що трапляются досить часто. Також це дозволяє запобігти, або хоча б знизити ризик кіберінциденту в неробочий час, реагуючи на аномалії, що виявляются автоматично тоді, коли за системою ніхто не спостерігає.

Для створення такої системи ми також можемо використовувати Splunk. Ось кілька прикладів того, як Splunk можна використовувати для автоматизованого реагування на кібератаки:

- Автоматичне блокування IP-адрес: Splunk може автоматично блокувати IP-адреси, з яких йде підозріла активність.
- Автоматичне ізолювання заражених комп'ютерів: Splunk може автоматично ізолювати заражені комп'ютери від мережі, щоб запобігти поширенню інфекції.
- Автоматичне розгортання патчів: Splunk може автоматично розгортати патчі безпеки для систем, які є вразливими до кібератак.
- Автоматичне сповіщення: Splunk може автоматично сповіщати фахівців з кібербезпеки про кібератаки.

Настройка Splunk для системи автоматизованого реагування на кібератаки може включати такі кроки:

1) Збір та моніторинг даних: Переконайтеся, що всі дані, які можуть бути пов'язані з кібератаками (логи, мережеві дані, дані безпеки тощо), надходять до Splunk.

2) Створення пошукових запитів: Створіть пошукові запити, щоб виявити потенційні загрози. Використовуйте SPL для пошуку аномальних патернів, незвичайної активності або вразливостей у вашій мережі.

3) Налаштування алертів: Створіть сповіщення або алерти, які спрацьовують при виявленні підозрілих подій або кібератак. Налаштуйте їх так, щоб вони надсилалися операторам або автоматично активували заходи захисту.

4) Впровадження кореляції подій: Налаштуйте кореляцію подій для виявлення складних кібератак, що використовують кілька шарів оборони або атакують різні точки в мережі.

5) Інтеграція з іншими інструментами безпеки: Підключіть Splunk до інших інструментів безпеки (наприклад, сім'ями безпеки, системами виявлення вторгнень тощо), щоб отримувати більш повне розуміння кіберзагроз і реагувати на них ефективніше.

6) Автоматизована реакція: Налаштуйте автоматизовані відповіді на виявлені загрози або кібератаки. Це може включати автоматичне блокування підозрілих IP-адрес або виконання інших заходів захисту.

3.3. Рекомендації щодо застосування розроблених методів та систем

3.3.1. Вибір методу

Вибір методу виявлення аномалій є критичним етапом у забезпеченні ефективного захисту інформаційних систем. Оскільки не існує універсального методу, який би підходив для всіх випадків, важливо враховувати специфіку завдання, тип даних та наявні ресурси. Розглянемо кілька ключових аспектів, які слід врахувати при виборі методу.

1. Характеристика даних:

- Тип даних: Для структурованих даних, таких як записи в базах даних, можуть підійти методи статистичного аналізу або традиційні алгоритми машинного навчання. Для неструктурованих даних, таких як текст, зображення чи відео, краще використовувати методи глибокого навчання.
- Розмір даних: Для великих обсягів даних слід використовувати методи, які можуть ефективно масштабуватися, наприклад, алгоритми, що працюють на розподілених системах.
- Шум у даних: Якщо дані містять багато шуму, важливо обрати методи, стійкі до шуму, наприклад, робастні статистичні методи або алгоритми з вбудованими механізмами фільтрації шуму.

2. Методи виявлення аномалій:

- Статистичні методи: Використовуються для виявлення аномалій на основі статистичних властивостей даних. Підходять для простих випадків із відомими розподілами даних.
- Методи машинного навчання: Поділяються на контрольовані та неконтрольовані. Контрольовані методи потребують навчальних даних із мітками, тоді як неконтрольовані методи працюють на даних без міток. Приклади: класифікація, кластеризація, методи на основі щільності (наприклад, DBSCAN).
- Методи глибокого навчання: Використовуються для складніших задач, що включають аналіз великих обсягів неструктурованих даних. Приклади: автоенкодери, рекурентні нейронні мережі (RNN), згорткові нейронні мережі (CNN).

3. Ресурси та інфраструктура:

- Обчислювальні ресурси: Деякі методи, особливо глибокого навчання, вимагають значних обчислювальних потужностей та спеціалізованого апаратного забезпечення (наприклад, GPU).
- Часові ресурси: Навчання складних моделей може займати багато часу. Варто враховувати, чи є можливість витратити цей час на навчання та налаштування моделі.

- Людські ресурси: Наявність кваліфікованих фахівців, які мають досвід роботи з обраними методами, є важливим фактором при виборі підходу.

4. Оцінка та вибір методу:

Крос-валідація: Використання методів крос-валідації для оцінки ефективності різних моделей на наявних даних.

Порівняння метрик: Оцінка методів за допомогою різних метрик, таких як точність, відсоток помилок, час виконання, використання ресурсів тощо.

Реальні умови: Тестування моделей у реальних умовах, щоб перевірити їхню здатність до виявлення аномалій у практичних сценаріях.

Підсумовуючи, вибір методу виявлення аномалій повинен базуватися на ретельному аналізі завдання, характеристик даних та наявних ресурсів. Рекомендується експериментувати з кількома методами та оцінювати їхню ефективність, щоб знайти найбільш підходящий для конкретного випадку.

3.2.2. Налаштування методу

Більшість методів виявлення аномалій мають ряд параметрів, які можна налаштувати залежно від конкретного випадку застосування. Оптимальне налаштування цих параметрів є ключовим для досягнення найкращих результатів. Рекомендується докладно ознайомитися з документацією до методу, який ви використовуєте, а також провести експерименти з різними значеннями параметрів для визначення оптимальних налаштувань.

При налаштуванні методу слід звертати увагу на такі аспекти як:

- Розмір вибірки: Деякі методи можуть вимагати певного розміру вибірки для ефективної роботи. Варто експериментувати з різними обсягами даних, щоб з'ясувати оптимальний розмір.
- Чутливість до аномалій: Деякі параметри впливають на чутливість методу до аномалій. Налаштування цих параметрів дозволяє контролювати рівень сприйнятливості методу до різних типів аномалій.

- Час навчання та виконання: Враховуйте обчислювальну складність методу та його час виконання при великих обсягах даних. Деякі параметри можуть впливати на час навчання та швидкість виконання алгоритму.

Важливо проводити експерименти з різними налаштуваннями параметрів та оцінювати їхній вплив на результати виявлення аномалій. Ретельне налаштування методу дозволить досягти оптимальної продуктивності та точності виявлення аномалій у вашій системі.

3.2.3. Тестування методу

Перед впровадженням методу на реальних даних рекомендується провести його тестування на спеціально підготовлених тестових даних. Цей етап дозволяє оцінити ефективність методу та визначити його обмеження перед його використанням в практичних умовах.

Під час тестування методу слід звернути увагу на наступні аспекти:

- Відтворюваність результатів: Переконайтеся, що результати тестування можуть бути відтворені. Використання фіксованих наборів тестових даних та стандартизованих метрик допоможе забезпечити об'єктивність та порівнюваність результатів.
- Оцінка продуктивності: Вимірюйте швидкодію та ресурсоємність методу під час тестування. Це дозволить вам оцінити його використання в реальному часі та визначити, чи відповідає він вашим вимогам до продуктивності.
- Оцінка точності: Використовуйте метрики оцінки результатів для оцінки точності методу. Порівнюйте результати його роботи з відомими аномаліями та нормальними зразками даних.

Правильне тестування методу дозволить вам зробити обґрунтований вибір щодо його використання вреальних умовах та підготувати його до успішної імплементації.

3.2.4. Моніторинг результатів

Після впровадження методу в реальному середовищі виникає необхідність систематично відслідковувати його результати. Це дозволяє виявляти ефективність методу та вчасно реагувати на будь-які аномалії чи проблеми. Моніторинг результатів також допомагає зрозуміти, як метод впливає на загальну безпеку системи та даних.

Основні аспекти моніторингу включають аналіз ефективності методу, виявлення нових видів аномалій та вчасну реакцію на потенційні проблеми. Цей процес дозволяє постійно вдосконалювати метод та адаптувати його до змінюючогося середовища.

Моніторинг та оптимізація є невід'ємною частиною стратегії кібербезпеки, яка допомагає підтримувати високий рівень захисту в умовах постійно змінюючихся загроз. Цей процес забезпечує надійний захист системи та зменшує ймовірність виникнення критичних інцидентів.

3.3.5. Оновлення методу

Після розгортання методу виявлення аномалій важливо пам'ятати про необхідність його регулярного оновлення. Оновлення методу дозволяє адаптувати його до змінюваних умов та вимог, що виникають у процесі експлуатації системи. Це може включати в себе вдосконалення алгоритмів, додавання нових функцій або модифікацію параметрів для забезпечення оптимальної ефективності.

Регулярний огляд та оновлення методів є ключовими складовими стратегії кібербезпеки, оскільки вони дозволяють вчасно реагувати на нові загрози та виклики. Недбалість у цьому аспекті може призвести до зниження ефективності методу та збільшення ризику безпеки. Тому рекомендується включати оновлення методів в план регулярних аудитів та перевірок безпеки.

3.3.6 Загальні рекомендації

- Використовуйте комбінацію методів для кращого виявлення аномалій.
- Використовуйте візуалізації даних для аналізу аномалій.
- Співпрацюйте з фахівцями з кібербезпеки для інтерпретації аномалій.
- Забезпечте відповідне навчання та підвищення кваліфікації персоналу.
- Регулярно переглядайте та оновлюйте свою систему виявлення аномалій.

Для забезпечення ефективного захисту хмарних систем від кібератак важливо дотримуватись ряду загальних рекомендацій, що охоплюють різні аспекти інформаційної безпеки. Однією з ключових рекомендацій є розробка та впровадження політик безпеки, які регулюють використання хмарних сервісів та забезпечують безпеку зберігання та обробки даних, а також моніторинг і реагування на інциденти.

Додатково, для забезпечення надійної аутентифікації та авторизації варто впровадити многофакторну аутентифікацію (MFA) та використовувати передові засоби управління ідентифікацією та доступом (IAM). Це дозволить ефективно контролювати доступ користувачів до ресурсів та знизити ризик несанкціонованого доступу.

Крім того, важливо застосовувати сучасні методи шифрування для захисту конфіденційної інформації, як у спокої, так і під час передачі. Це включає в себе використання надійних алгоритмів шифрування та впровадження спеціалізованих рішень для управління ключами шифрування, таких як апаратні модулі безпеки (HSM).

До цього ж, для забезпечення безпеки на рівні мережевої інфраструктури, рекомендується встановлення та налаштування фаєрволів для контролю трафіку, а також використання віртуальних приватних мереж (VPN) для забезпечення захищеного доступу до хмарних ресурсів. Це дозволяє ефективно захистити мережеві комунікації та запобігти несанкціонованому доступу до даних.

Крім того, для захисту від DDoS-атак варто впровадити спеціалізовані хмарні сервіси, такі як AWS Shield, Cloudflare або Akamai, які надають захист від

різних видів кібератак. Додатково, регулярний моніторинг мережевого трафіку для виявлення аномалій та потенційних DDoS-атак допоможе своєчасно виявити та відвернути загрози.

Використання захисту на рівні додатків є також важливим аспектом безпеки. Рекомендується використовувати веб-фаєрволи (WAF) для захисту веб-додатків від різних атак, таких як SQL-ін'єкції та XSS, а також регулярно сканувати вразливості для виявлення потенційних проблем безпеки.

Загалом, впровадження зазначених рекомендацій допоможе організаціям підвищити рівень захисту хмарних систем, знизити ризики кібератак та забезпечити безпеку даних та інфраструктури.

Для ефективного реагування на потенційні загрози та інциденти безпеки важливо використовувати централізоване логування та моніторинг, яке дозволяє збирати та аналізувати дані про активність усіх систем та ресурсів. Також необхідно використовувати сучасні системи виявлення аномалій, які забезпечують реагування на непередбачені події у режимі реального часу. Штучний інтелект може бути використаний для аналізу аномалій та прогнозування потенційних загроз, а також для автоматизації процесів реагування на інциденти, що дозволяє швидко та ефективно нейтралізувати загрози безпеки.

Крім цього, важливо проводити регулярні аудити безпеки для оцінки стану захищеності хмарних систем та виявлення потенційних вразливостей. Також рекомендується залучати спеціалістів для проведення тестування на проникнення з метою виявлення слабких місць та проблем безпеки та їх подальшого виправлення. Регулярні аудити та тестування допомагають підтримувати високий рівень безпеки та впевненість у стійкості хмарних систем до кіберзагроз.

Висновки до розділу 3

Розроблені методи та засоби захисту хмарних систем на основі штучного інтелекту є перспективним напрямком розвитку захисту інформації. Ці методи та засоби можуть використовуватися для захисту хмарних систем у різних сферах, включаючи захист критичної інфраструктури, персональних даних та фінансових систем.

Використання штучного інтелекту у сфері безпеки хмарних систем дозволяє значно підвищити ефективність виявлення та запобігання загрозам. Завдяки адаптивним алгоритмам машинного навчання, системи захисту можуть швидко реагувати на нові типи атак, аналізувати великі обсяги даних у реальному часі та автоматично адаптуватися до змін у середовищі загроз.

Дослідження показало, що впровадження методів штучного інтелекту у хмарні системи безпеки дозволяє:

Підвищити рівень автоматизації процесів захисту: Автоматизація дозволяє значно скоротити час реакції на загрози та зменшити навантаження на людські ресурси.

Забезпечити більш точну ідентифікацію загроз: Алгоритми машинного навчання здатні аналізувати складні патерни поведінки та виявляти аномалії, які можуть свідчити про потенційні атаки.

Поліпшити управління доступом та автентифікацію: Використання біометричних даних та поведінкових біометричних характеристик для аутентифікації користувачів підвищує рівень безпеки доступу до хмарних ресурсів

Оптимізувати процеси реагування на інциденти: Завдяки інтеграції інтелектуальних систем виявлення та реагування на інциденти, хмарні системи можуть швидше та більш ефективно усувати наслідки атак.

Забезпечити безперервний моніторинг та аналіз безпеки: Постійний моніторинг хмарних систем у режимі реального часу дозволяє виявляти та нейтралізувати загрози ще на ранніх стадіях.

Результати дослідження демонструють, що використання штучного інтелекту в хмарних системах безпеки є ключовим фактором для забезпечення надійного захисту даних та ресурсів в умовах постійного зростання складності та кількості кіберзагроз. Подальший розвиток та вдосконалення цих технологій відкриває нові можливості для захисту інформації та підтримання кібербезпеки на високому рівні.

ВИСНОВКИ

Проведено дослідження застосування алгоритмів Штучного Інтелекту для захисту хмарних систем.

Встановлено, що Штучного Інтелекту може значно покращити безпеку хмарних систем за рахунок виявлення аномальних патернів та прогнозування кібератак.

Розглянуто три варіанти Методів Штучного Інтелекту, що використовуються: Система виявлення аномалій, Система прогнозування кібератак та Система автоматизованого реагування на кібератаки.

Проаналізовано різні алгоритми Штучного Інтелекту, які можуть використовуватися для захисту хмарних систем, такі як алгоритми класифікації, кластеризації та аномального виявлення.

Описано інструменти та засоби, які можуть використовуватися для реалізації систем захисту хмарних систем на основі Штучного Інтелекту.

Наведено рекомендації щодо використання Штучного Інтелекту для захисту хмарних систем в конкретних сферах.

Встановлено, що використання Штучного Інтелекту є перспективним напрямком покращення безпеки хмарних систем.

Рекомендовано продовжити дослідження в цій галузі для розробки більш ефективних та точних систем захисту на основі Штучного Інтелекту.

Отримані результати можуть бути використані науковцями та практиками для розробки нових методів та систем захисту хмарних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology (NIST) Cybersecurity Framework. URL: https://www.nist.gov/cybersecurity
2. Cloud Security Alliance (CSA) Cloud Controls Matrix. URL: https://cloudsecurityalliance.org/research/cloud-controls-matrix
3. ENISA Cloud Computing Security Guidelines. URL: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
4. Traffic-Sign-Recognition-with-Keras-Tensorflow.URL: github.com/nguyenrobot/Traffic-Sign-Recognition-with-Keras-Tensorflow/blob/main/README.md
5. URL: louis.uah.edu/cgi/viewcontent.cgi?article=1200&context=uah-dissertations
6. "LOF: Виявлення локальних викидів" URL: https://scikit-learn.org/stable/auto_examples/neighbors/plot_lof_outlier_detection.html
7. "Огляд методів виявлення аномалій" URL: https://www.sciencedirect.com/topics/computer-science/anomaly-detection
8. Scikit-learn. URL: https://scikit-learn.org/
9. Документація Splunk. URL: https://docs.splunk.com/
10. Навчання Splunk URL: https://www.splunk.com/training/
11. Офіційний сайт Splunk. URL: https://www.splunk.com/
12. Стаття на Хабр: https://habr.com/ru/articles/160197/
13. 4 питання щодо кібербезпеки при впровадженні ШІ.URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/4-cybersecurity-considerations-for-ai-deployment
14. Аналіз вразливостей хмарних технологій.URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/06/51-2.pdf
15. Ризики інформаційної безпеки в хмарних сервісах.URL: https://openarchive.nure.ua/bitstreams/738384c8-f397-4ae7-b034-75789907d96c/download

16. Attribution of multi-annual to decadal changes in the climate system: the large ensemble single forcing model intercomparison project (LESFMIP) / D. M. Smith et al. Frontiers in climate. 2022. Vol. 4. URL: https://doi.org/10.3389/fclim.2022.955414

17. Junqueira R. Mário santiago de carvalho, A síntese frágil. edição digital publicada pelo instituto de estudos filosóficos da faculdade de letras da universidade de coimbra, 2022. DOI: https://doi.org/10.5281/zenodo.6345442. Revista filosófica de coimbra. 2024. Vol. 33, no. 65. P. 188–189. URL: https://doi.org/10.14195/0872-0851_65_14

18. Zhang B, et al. (2024) A comparative study to investigate the individual contribution of metabolic and physical interaction on volatiles formation in the mixed fermentation of Torulaspora delbrueckii and Saccharomyces cerevisiae. Food Microbiol 119: 104460. URL: https://www.yeastgenome.org/reference/S000347260

19. Платформа ідентифікації Auth0 URL:https://auth0.com/docs

20. Офіційна документація Okta: https://www.okta.com/documentation/

21. Важливість налаштування гіперпараметрів у машинному навчанні https://towardsdatascience.com/understanding-hyperparameters-and-its-optimisation-techniques-f0debba07568

22. Вступ до налаштування гіперпараметрів **https://github.com/google-research/tuning_playbook**

23. Налаштування гіперпараметрів: Посібник **https://pyimagesearch.com/2021/05/17/introduction-to-hyperparameter-tuning-with-scikit-learn-and-python/**

24. Важливість тестування моделей машинного навчання https://towardsdatascience.com/things-no-one-tells-you-about-testing-machine-learning-28b7a3df3bca

25. Посібник з тестування моделей машинного навчання https://cloud.google.com/products/ai

26. Як тестувати моделі машинного навчання: Повний посібник https://analyticsindiamag.com/

27. Важливість моніторингу моделей машинного навчання https://towardsdatascience.com/monitoring-your-machine-learning-model-6cf98c106e99

28. Посібник з моніторингу моделей машинного навчання. URL: https://cloud.google.com/products/ai

29. Як моніторити моделі машинного навчання у виробництві. URL: https://developer.nvidia.com/blog/a-guide-to-monitoring-machine-learning-models-in-production/

30. Важливість оновлення моделей машинного навчання. URL: https://towardsdatascience.com/machine-learning/home

31. Посібник з оновлення моделей машинного навчання. URL: https://cloud.google.com/products/ai

32. Як оновлювати моделі машинного навчання у виробництві. URL: https://www.youtube.com/watch?v=50GB6FEGBZQ

33. Виявлення аномалій для кібербезпеки: Повний огляд. URL: https://arxiv.org/abs/2105.06742

34. Multi-factor authentication MFA URL: https://en.wikipedia.org/wiki/Help:Two-factor_authentication

35. Role-based access control RBAC URL: https://en.wikipedia.org/wiki/Role-based_access_control

36. Identity and access management IAMhttps://en.wikipedia.org/wiki/Identity_management

37. Firewalls URL: https://en.wikipedia.org/wiki/Firewall_%28computing%29)

38. Intrusion detection systems URL: IDShttps://en.wikipedia.org/wiki/Intrusion_detection_system

39. Intrusion prevention systems URL: IPShttps://en.wikipedia.org/wiki/Intrusion_detection_system

40. Antivirus software URL: https://en.wikipedia.org/wiki/Antivirus_software)

41. Virtual private networks URL: VPNshttps://en.wikipedia.org/wiki/Virtual_private_network

42. Data encryption URL: https://en.wikipedia.org/wiki/Encryption

43. Machine learning URL: https://en.wikipedia.org/wiki/Machine_learning

44. Anomaly detection URL: https://en.wikipedia.org/wiki/Anomaly_detection

45. Cyberattack prediction URL: https://en.wikipedia.org/wiki/Cyberattack