ВЫЯВЛЕНИЕ УГРОЗ И РЕАГИРОВАНИЕ НА НИХ В ОБЛАЧНОЙ БЕЗОПАСНОСТИ: ОБЗОР СТРАТЕГИЙ, ОСНОВАННЫХ НА ИСКУССТВЕННОМ ИНТЕЛЛЕКТЕ

Алекедзро Кодзови Арман, аспирант

Труфанов Андрей Иванович, канд. физ.-мат. наук, доцент

Иркутский Национальный Исследовательский Технический Университет

(Россия, г. Иркутск)

Аннотация. *Облачные вычисления существенно преобразовали цифровую среду, предоставив масштабируемые вычислительные ресурсы, гибкость инфраструктуры и снижение эксплуатационных расходов. Тем не менее, распределённая архитектура и модель совместного использования ресурсов несколькими пользователями создают серьёзные проблемы безопасности. Традиционные методы обнаружения угроз, основанные на фиксированных сигнатурах, статических правилах и ручном анализе, становятся не столь эффективными по мере усложнения кибератак, направленных на современные облачные системы.*

В последние годы для решения этих проблем активно внедряются технологии искусственного интеллекта. Использование методов машинного обучения, глубокого обучения и обучения с подкреплением позволяет выявлять аномалии, анализировать события в реальном времени и автоматизировать процессы защиты, минимизации ущерба и ликвидации последствий кибератак . Такие системы способны постоянно обучаться на новых данных, что повышает точность обнаружения атак и уменьшает количество ложных срабатываний.

Дополнительные возможности появляются благодаря интеграции крупных языковых моделей с платформами управления безопасностью. Это позволяет эффективно реагировать на инциденты, автоматически изолировать заражённые ресурсы, а также реализовывать механизмы самовосстановления инфраструктуры. В работе раскрываются современные методы обнаружения и реагирования на угрозы, анализируются их преимущества и ограничения, а также обсуждаются

проблемы конфиденциальности данных, уязвимости алгоритмов машинного обучения , сложности и ошибки интеграции таких решений. Полученные результаты показывают, что дальнейшее развитие систем безопасности облачных сред будет тесно связано с использованием автономных и масштабируемых решений на основе искусственного интеллекта.

***Ключевые слова**: облачные вычисления , безопасность, угрозы, инциденты, автоматизированное реагирование, искусственный интеллект, машинное обучение*

Введение

Современные подходы предоставляют возможность доступа по требованию к общим информационным ресурсам, включая хранилище данных, приложения и вычислительные мощности. Они стали существенными для частных пользователей, государственных организаций и бизнеса за счёт своей гибкости, масштабируемости и экономической эффективности. Облачные вычисления выступают ключевым компонентом нынешней цифровой инфраструктуры.

Не всегда полностью учитывая связанные с этим уязвимости безопасности. Уязвимость облачной инфраструктуры к атакам объясняется тем, что динамическая природа облачной среды, мультиарендность и распределённая архитектура предоставляют злоумышленникам больше возможностей для её компрометации. Поэтому устойчивость облачных вычислений играет важную роль в формировании доверия и надёжности в виртуальной экосистеме. Предприятия переносят критически важные данные и сервисы в облако

Которые могут негативно повлиять на конфиденциальность, доступность и целостность информации, относятся утечки данных, инсайдерские угрозы, внедрение вредоносного программного обеспечения, атаки отказа в обслуживании и несанкционированный возможность доступа [8]. Одним из

ключевых элементов облачной безопасности представляет собой обнаружение угроз .

Основанных на фиксированных правилах и сопоставлении сигнатур [10]. кроме того, масштаб и разнообразие облачного сетевого трафика делают ручной мониторинг более сложным, поскольку он требует значительных ресурсов и может приводить к ошибкам [11][12]. Это привело к разработке новых архитектур обнаружения угроз, способных выявлять аномалии, уменьшать количество ложных срабатываний и обеспечивать ситуационную осведомлённость в режиме реального времени. Постоянно растущая сложность атак на облачные системы формирует серьёзные трудности для традиционных методов обнаружения но и способность быстро локализовать и минимизировать последствия такой активности [13][14]. Реагирование на угрозы также играет важную роль в снижении ущерба от киберинцидентов [15][16]. Обнаружение и реагирование на угрозы в облачной безопасности подразумевает не только способность выявлять вредоносную активность.

Что не всегда достаточно быстро при массовых или происходящих в реальном времени атаках [17][18]. Поэтому всё чаще применяются автоматизированные механизмы реагирования, позволяющие ускорить процесс реагирования за счёт изоляции затронутых ресурсов, внедрения правил безопасности и предотвращения дальнейшего распространения атак внутри системы. Автоматизация представляет собой одним из ключевых решений для создания устойчивой и гибкой облачной инфраструктуры. Традиционные модели реагирования часто требуют участия человека.

Применяя методы машинного обучения (ml), глубокого обучения (dl) и обучения с подкреплением (rl), способны анализировать большие объёмы разнородных данных облачной среды, выявлять новые векторы атак и автоматически инициировать защитные действия. Искусственный интеллект стал ключевым элементом повышения эффективности обнаружения и реагирования на угрозы в облачных средах .

Ии гарантирует возможности прогнозной аналитики, адаптивного применения политик безопасности и непрерывного самообучения, что

делает систему более устойчивой к изменяющимся угрозам . объединяя данные журналов событий, действия пользователей и сетевой трафик, системы ии помогают уменьшить количество ложных срабатываний и повысить уровень ситуационной осведомлённости .

Помимо реактивной безопасности Системы реагирования на основе ии способны в режиме реального времени расставлять приоритеты и координировать контрмеры, что открывает путь к масштабируемым, саморегулирующимся и автономным системам безопасности облачных сред.

2. Безопасность облаков и ландшафт угроз

Гибкости и низким эксплуатационным затратам. однако их распределённая и мультиарендная природа формирует сложную среду угроз, требующую специализированных мер безопасности. развитие облачных вычислений значительно изменило способы управления информационными технологиями в организациях, сделав общие вычислительные ресурсы постоянно доступными через интернет (рисунок 1). Облачные вычисления стали неотъемлемой частью современных цифровых сервисов за счёт своей масштабируемости.

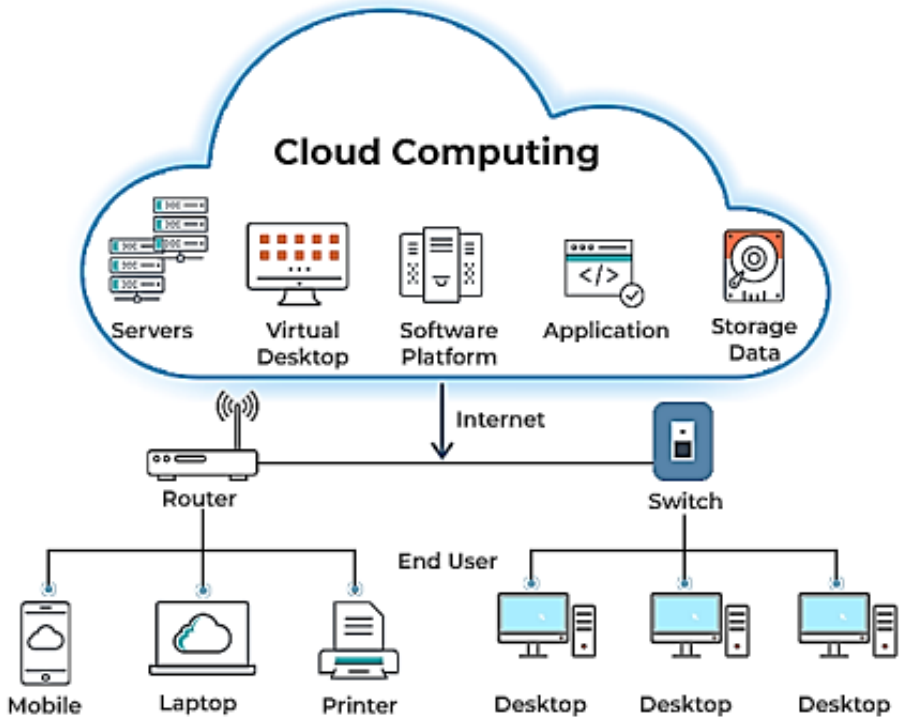

Рис. 1: Архитектура облачных вычислений

Обработку и возможность доступа через интернет-соединение. Она включает хранилища данных, приложения, программные платформы, виртуальные рабочие столы и серверы. Эта модель вычислений использует удалённое хранение данных.

2.1. Модели и архитектуры облачных вычислений

Позволяющие пользователям получать возможность доступа к общим вычислительным ресурсам по требованию. эти модели определяют способы предоставления, управления и использования сервисов в облачной экосистеме. Облачные вычисления предлагают различные сервисные модели и архитектуры развертывания.

2.1.1. Модель сервисов

Однако наиболее распространёнными выступают три основные модели: saas, iaas и paas, которые также называются моделями облачных сервисов.

В настоящее время облачные вычисления предоставляют широкий спектр услуг.

2.1.2. Infrastructure as a Service (IaaS)

Вычислительные ресурсы в основном состоят из аппаратных и программных компонентов. Они выступают основой любой вычислительной системы.

Iaas дает возможность пользователям получать возможность доступа к инфраструктуре без необходимости приобретения и обслуживания собственного оборудования. В облачной среде эти ресурсы предоставляются пользователям через модель Infrastructure as a Service (IaaS).

Примеры IaaS : Microsoft Azure, AWS, Cisco Metacloud

Platform as a Service (PaaS)

Модель PaaS предоставляет разработчикам возможность создавать собственные приложения без необходимости настраивать среду разработки. Она использует API, языки программирования и промежуточное программное обеспечение.

Примеры PaaS : AWS Elastic Beanstalk , Apache Stratos, Google App Engine, Microsoft Azure.

Software as a Service (SaaS)

Модель SaaS позволяет пользователям получать доступ к программному обеспечению и сервисам через интернет по подписке или по мере необходимости. Для работы с такими приложениями обычно требуется только веб-браузер или тонкий клиент.

Это снижает нагрузку на аппаратные ресурсы пользователя и обеспечивает централизованное управление, развертывание и обслуживание программного обеспечения.

Примеры SaaS: Microsoft Office 365,Salesforce,Cisco WebEx,Google Apps

Модели развертывания облака

Организации часто сталкиваются с выбором между тремя основными моделями облачного развертывания: публичное облако, частное облако и гибридное облако .

Публичное облако

Обмена файлами и хранения неконфиденциальных данных. публичные облака также часто используются для разработки программного обеспечения. Публичное облако представляет собой одной из наиболее распространённых моделей облачных вычислений. Оно широко используется для веб-приложений.

Частное облако

Также называемое внутренним или корпоративным облаком, предоставляет инфраструктуру, предназначенную исключительно для одной организации. обычно оборудование размещается в собственных центрах обработки данных компании.

Гибридное облако

Гибридные облака объединяют публичные и частные облачные среды. Их архитектура гарантирует плавное перемещение данных и приложений между различными платформами. Такая модель подходит организациям различных размеров и отраслей.

2.1.3. Архитектурные основы облачных систем

Ключевые элементы архитектуры облачных систем включают:

2.1.3.1. Виртуализация и контейнеризация

Облачные вычисления основаны на технологиях виртуализации и контейнеризации, которые обеспечивают эффективное использование ресурсов, масштабируемость и изоляцию.

Виртуализация

- Виртуализация позволяет нескольким рабочим нагрузкам использовать одну физическую инфраструктуру.

- Гипервизор управляет виртуальными машинами и распределяет ресурсы между ними.
  Популярные гипервизоры включают VMware, Hyper-V и KVM.
- Виртуализация обеспечивает гибкость, изоляцию ошибок и независимость от аппаратного обеспечения, однако она обычно требует больше ресурсов, чем контейнеризация.

Контейнеризация

Контейнеры запускаются быстрее и используют меньше ресурсов, чем виртуальные машины, поскольку они используют ядро операционной системы хоста.

2.1.3.2. Мультиарендность

Эффективность и экономичность saas-приложений. Мультиарендность в облачных средах значительно повышает масштабируемость

Использование общих ресурсов несколькими арендаторами дает возможность поставщикам SaaS уменьшить операционные расходы на одного клиента и максимально эффективно использовать инфраструктуру.

2.1.3.3. Эластичность и масштабируемость

Что дает возможность оптимизировать затраты и избегать избыточного выделения ресурсов., Эластичность означает способность облачных систем автоматически выделять или освобождать ресурсы в зависимости от текущего спроса

В свою очередь, означает способность системы справляться с увеличением нагрузки за счёт расширения ресурсов отдельных машин или всей системы, Масштабируемость.

2.2. Угрозы и уязвимости в облачных средах

Которое может нанести ущерб системе или организации. система или актив считаются уязвимыми, если в них существуют слабые места, которые могут быть использованы угрозой. Злоумышленник может инициировать атаку, применяя такие уязвимости. Угроза это событие или действие.

2.2.1. Утечки данных

Когда неавторизованное лицо или группа получают возможность доступа, копируют или передают конфиденциальную информацию, принадлежащую человеку или организации. утечки данных выступают одной из наиболее серьёзных и распространённых угроз в облачных вычислениях.

2.2.2. Потеря данных

Включая природные катастрофы (например, наводнения или землетрясения), человеческие ошибки, случайное удаление данных администраторами облака, отказ оборудования, перебои в электроснабжении или вредоносное программное обеспечение. Потеря или повреждение данных могут происходить по различным причинам.

2.2.3. Злонамеренные инсайдеры

Системных администраторов, подрядчиков или бизнес-партнёров, имеющих возможность доступа к инфраструктуре. Одной из наиболее серьёзных угроз выступают злонамеренные инсайдеры. Потенциальные внутренние угрозы могут исходить от сотрудников.

2.2.4. Атаки отказа в обслуживании (DoS)

Перегружая её запросами. такие атаки могут быть усилены использованием ботнетов, что делает их особенно опасными. Атака отказа в обслуживании (DoS) влияет на доступность системы.

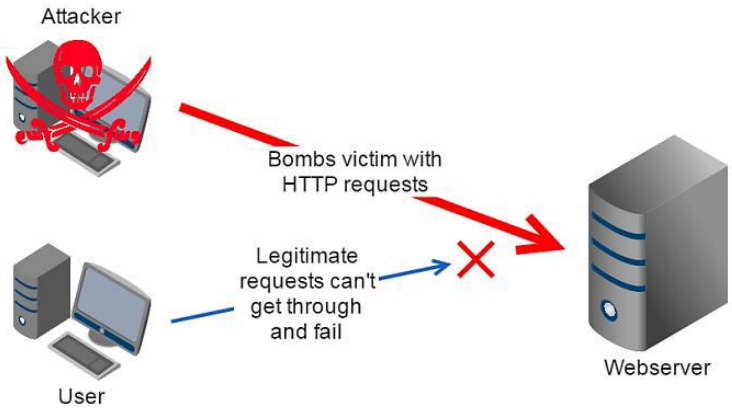

Рис. 2: Отказ в обслуживании

2.2.5. Уязвимые системы и API

Он может получить возможность доступа к облачным ресурсам. Облачные приложения часто используют API для взаимодействия с пользователями. Если злоумышленник успешно использует уязвимость в API.

2.2.6. Захват учётных записей

Когда злоумышленник получает возможность доступа к действительной учётной записи пользователя и использует её для вредоносных действий. Захват учётной записи происходит.

2.2.7. Продвинутые постоянные угрозы (APT)

Вредоносного кода, сетевых атак и других методов. APT-атаки направлены на получение долгосрочного доступа к облачной инфраструктуре и кражу данных. Они могут осуществляться с помощью фишинга.

2.3. Традиционные методы обнаружения и реагирования на угрозы

Правилах и ручном анализе специалистами. В традиционных системах кибербезопасности обнаружение угроз основано на сигнатурах.

2.3.1. Обнаружение на основе сигнатур

Но плохо справляются с новыми атаками., Такие системы сравнивают наблюдаемую активность с известными сигнатурами вредоносного программного обеспечения. Они эффективны против известных угроз

2.3.2. Защита на основе правил

Брандмауэры и списки контроля доступа используют заранее определённые правила для ограничения несанкционированного доступа. Однако такие методы плохо адаптируются к динамическим облачным средам.

2.3.3. Ручное реагирование на инциденты

Команды безопасности должны вручную анализировать и устранять инциденты. Этот процесс требует времени и может приводить к ошибкам.

3. Обнаружение угроз в облачных системах с использованием ИИ

3.1. Подходы машинного обучения

Методы машинного обучения используют модели для анализа и классификации шаблонов данных.

3.2. Контролируемое обучение

Алгоритмы обучаются на размеченных данных. Они широко используются в кибербезопасности для классификации сетевого трафика.

Примеры алгоритмов:

* Decision Tree

* Naïve Bayes

3.2.1. Неконтролируемое обучение

Эти алгоритмы не требуют размеченных данных и используются для выявления аномалий.

Методы:

* Clustering

* PCA

* Autoencoders

3.2.2. Обучение с подкреплением

Который дает возможность системам принимать решения в динамических средах.

Примеры:

* Q-learning

* Deep Q-Networks

3.3. Глубокое обучение

Глубокое обучение позволяет анализировать сложные и многомерные данные.

Примеры методов:

* Bayesian networks

* LSTM

* Neural networks

3.4. Системы обнаружения вторжений (IDS)

IDS контролируют сетевой трафик и системные события для выявления вредоносной активности .

3.5. Проблемы использования ИИ

Основные проблемы:

* сложность интеграции

* защита конфиденциальности данных

* зависимость от качества данных

* атаки на модели машинного обучения

* высокая стоимость внедрения

4. Стратегии автономного реагирования на угрозы

Автономные системы безопасности позволяют автоматически обнаруживать и нейтрализовать угрозы с минимальным участием человека.

4.1. Автоматизированное управление инцидентами

Жизненный цикл реагирования на инциденты критически важен. Без чёткой структуры команды теряют время, не понимают, кто за что отвечает, а угрозы успевают распространиться. Наличие слаженной команды реагирования (IR) экономит около 248 000 долларов в год, а использование ИИ и автоматизации ускоряет обнаружение и сдерживание атак на 98 дней.

Главное цикл не заканчивается: каждый инцидент идёт в пользу улучшения защиты.

Модель NIST включает четыре этапа. Первый подготовка: разрабатываются планы и сценарии (playbooks), назначаются роли, обучается команда, внедряются инструменты вроде EDR и SIEM, а также прописываются протоколы связи. Второй этап обнаружение и анализ: здесь сырые оповещения превращаются в полноценные инциденты. Специалисты сортируют события, оценивают их серьёзность, сопоставляют данные, собирают доказательства и определяют масштаб атаки.

Третий этап объединяет сдерживание, устранение и восстановление. Сначала идёт краткосрочная изоляция угрозы, затем долгосрочное сдерживание (сегментация сети). После этого полностью удаляются вредоносные программы и «чёрные ходы», а системы шаг за шагом восстанавливаются из чистых резервных копий. Четвёртый этап пост-инцидентный анализ: проводятся разборы ошибок, составляется детальный отчёт, обновляются процедуры, а полезная информация передаётся надёжным партнёрам.

Существует также модель SANS из шести шагов (подготовка, идентификация, сдерживание, устранение, восстановление, уроки). По сути, она повторяет NIST, просто детализирует шаги иначе. Главное иметь повторяемый и чёткий процесс, который обеспечивает быстрое обнаружение, скоординированную реакцию и постоянное улучшение после каждого инцидента

При этом специалисты допускают расширение четырех ступенчатой модели до 5-6 фаз (рис.3)

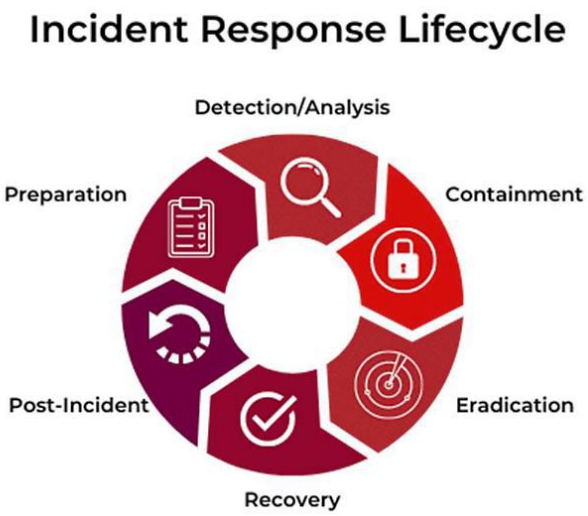

Рис. 3: Жизненный цикл реагирования на инциденты в угрозе

4.2. Политико-ориентированная защита

Политики безопасности автоматически применяются к системам и обновляются в реальном времени .

4.2.1. Обнаружение угроз в реальном времени

Используемые технологии:

* SIEM

* EDR

* SOAR

4.2.2. Адаптивное обновление политик

Вместо статичных правил, которые рано или поздно устаревают, современные облачные системы начинают действовать как живые организмы: они используют ИИ и аналитику угроз, чтобы постоянно подстраивать политики безопасности под меняющиеся атаки. Представьте, что система сама, в реальном времени, меняет настройки доступа, параметры файрвола и пороги аномалий так она может отразить даже то, с

чем раньше не сталкивалась, например, атаку zero-day. Благодаря непрерывному обучению такой подход не только повышает точность обнаружения угроз, но и снижает число ложных срабатываний, сохраняя защиту надёжной и гибкой в постоянно меняющемся облачном окружении.

5. Заключение и будущие исследования

В заключение следует отметить, что интеграция методов глубокого обучения и обработки естественного языка в облачные среды позволяет значительно повысить точность обнаружения угроз и ускорить процессы реагирования на инциденты. Искусственный интеллект сегодня играет ключевую роль в развитии систем кибербезопасности облачных инфраструктур благодаря использованию методов машинного обучения, способных анализировать большие объёмы данных и выявлять сложные вредоносные действия.

Полученные результаты показывают, что подходы, основанные на искусственном интеллекте, демонстрируют более высокую эффективность по сравнению с традиционными методами обнаружения угроз, особенно с точки зрения автоматизации, адаптивности и проактивного выявления атак. Такое сравнение подтверждает преимущества современных моделей глубокого обучения для повышения устойчивости и масштабируемости систем безопасности облачных инфраструктур.

Тем не менее, остаётся ряд серьёзных проблем. Одной из основных является обеспечение конфиденциальности данных, а также защита моделей машинного обучения от adversarial-атак. Кроме того, недостаточная интерпретируемость алгоритмов затрудняет понимание решений, принимаемых системами искусственного интеллекта, тогда как высокая стоимость внедрения ограничивает широкое применение подобных технологий.

В связи с этим будущие исследования должны быть направлены на разработку моделей искусственного интеллекта, обеспечивающих сохранение конфиденциальности данных, повышение интерпретируемости алгоритмов и устойчивость к атакам на модели машинного обучения. Также необходимо совершенствовать механизмы взаимодействия человека и

искусственного интеллекта для обеспечения более эффективного контроля и принятия решений. Реализация данных направлений позволит создать более автономные, масштабируемые и устойчивые системы безопасности облачных инфраструктур, способные эффективно противостоять современным и будущим киберугрозам.

Список литературы

[1] Abhishek and P. Khare, “Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development,” Int. J. Curr. Eng. Technol., vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.

[2] S. S. S. Neeli, “Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks,” J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, pp. 2102–2106, Nov. 2022, doi: 10.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[3] V. Shah, “An Analysis of Dynamic DDoS Entry Point Localization in Software-Defined WANs,” Int. J. Adv. Res. Sci. Commun. Technol., vol. 4, no. 6, pp. 442–455, Nov. 2024, doi: 10.48175/IJARSCT-22565.

[4] Maniah, E. Abdurachman, F. L. Gaol, and B. Soewito, “Survey on Threats and Risks in the Cloud Computing Environment,” Procedia Comput. Sci., vol. 161, pp. 1325–1332, 2019, doi: 10.1016/j.procs.2019.11.248.

[5] S. R. Kurakula, “Cloud-native microservices in financial services: Architecting for scalability and flexibility,” World J. Adv. Res. Rev., vol. 26, no. 02, pp. 1435–1442, 2025.

[6] J. Thomas, K. V. Vedi, and S. Gupta, “Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics,” J. Emerg. Technol. Innov. Res., vol. 8, no. 9, 2021.

[7] P. Pathak, A. Shrivastava, and S. Gupta, “A survey on various security issues in delay tolerant networks,” J Adv Shell Program., vol. 2, no. 2, pp. 12–18, 2015.

[8] N. Kaloudi and J. Li, “The AI-Based Cyber Threat Landscape: A Survey,” ACM Comput. Surv. vol. 53, no. 1, Feb. 2020, doi: 10.1145/3372823.

[9] S. Dodda, S. Chintala, N. Kunchakuri, and N. Kamuni, “Enhancing Microservice Reliability in Cloud Environments Using Machine Learning for Anomaly Detection,” in 2024 International Conference on Computing, Sciences and Communications (ICCSC), IEEE, Oct. 2024, pp. 1–5. Doi: 10.1109/ICCSC62048.2024.10830437.

[10] H. Sultana, “Machine Learning for Cybersecurity: Threat Detection and Prevention,” ShodhKosh J. Vis. Perform. Arts, vol. 5, no. 7, 2024, doi: 10.29121/shodhkosh.v5.i7.2024.4592

[11] N. Malali, “Using Machine Learning to Optimize Life Insurance Claim Triage Processes Via Anomaly Detection in Databricks: Prioritizing High-Risk Claims for Human Review,” Int. J. Eng. Technol. Res. Manag., vol. 6, no. 6, 2022, doi: 10.5281/zenodo.15176507.

[12] S. B. Karri, C. M. Penugonda, S. Karanam, M. Tajammul, S. Rayankula, and P. Vankadara, “Enhancing Cloud-Native Applications: A Comparative Study of Java-To-Go Micro Services Migration,” Int. Trans. Electr. Eng. Comput. Sci., vol. 4, no. 1, pp. 1–12, 2025.

[13] D. Patel and R. Tandon, “Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication,” Int. J. Adv. Res. Sci. Commun. Technol., pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[14] V. Shah, “Securing the Cloud of Things: A Comprehensive Analytics of Architecture, Use Cases, and Privacy Risks,” ESP J. Eng. Technol. Adv., vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[15] V. M. L. G. Nerella, “Observability-Driven SRE Practices for Proactive Database Reliability and Rapid Incident Response,” Int. J. Recent Innov. Trends Comput. Commun. vol. 7, no. 8, pp. 32–38, Aug. 2019, doi: 10.17762/ijritcc.v7i8.11710.

[16] V. M. L. G. Nerella, “Architecting Secure, Automated Multi-Cloud Database Platforms Strategies for Scalable Compliance,” Int. J. Intell. Syst. Appl. Eng., vol. 9, no. 1, pp. 128–138, 2021.

[17] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies,” IEEE Access, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[18] S. K. Chintagunta, “Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation,” TIJER – Int. Res. J., vol. 9, no. 10, pp. 49–55, 2022.