Golden Sun-Rise
International Journal of Multidisciplinary on Science and Management
ISSN: 3048-5037/ Volume 3 Issue 1 Jan-Mar 2026 / Page No: 18-27
Paper Id: IJMSM-V3I1P103/ Doi:10.71141/30485037/V3I1P103

Research Article

Incident Response and Disaster Recovery in Cloud Computing

Krishna Mohan Pitchikala

Software Development Engineer, Amazon, USA

Received: 02 January 2026 Revised: 04 January 2026 Accepted: 08 January 2026 Published: 12 January 2026

Abstract - *Cloud computing has transformed IT service delivery with a pay-as-you-go model that simplifies software creation, deployment, and maintenance. It has also reshaped how businesses handle security challenges, particularly in incident response (IR) and disaster recovery (DR). IR is a proactive approach to detecting, controlling, and mitigating security risks, while DR focuses on restoring systems after failures caused by cyberattacks, system errors, or natural disasters. Unlike traditional on-premises IT environments, where organizations have full control, cloud-based environments rely on third-party providers, introducing new processes and responsibilities for managing IR and DR. Cloud security is now a shared responsibility between providers and customers, requiring collaboration to ensure effective protection. This paper analyzes how cloud security management differs from traditional approaches, focusing on key principles and best practices for incident response and disaster recovery from a business perspective. It also examines a real-world cloud security breach to highlight the challenges businesses face in responding to incidents and recovering from disruptions. Additionally, it explores the latest advancements in automated disaster recovery, which enhance resilience and reliability. By understanding these concepts, businesses can strengthen their security posture, improve response strategies, and ensure seamless business continuity.*

Keywords - *Cloud Computing, Incident Response, Disaster Recovery, Cloud Security, Business Continuity, Shared Responsibility Model.*

I. INTRODUCTION

A computer is a physical machine that processes data, while software is a set of instructions and programs that tell the computer what to do. Think of it as hardware (the computer) requiring software (programs) to function. In software development, computing refers to the use of computers and software to create, test, and run applications. Computing in the context of the software development is the field where computers and software are used to write, test, and execute programs. The process involves code writing, data manipulation, calculations as well as command execution to accomplish tasks or solve problems. Cloud computing has made it easy to start and operate a business today. Businesses can utilize third party firms cloud services at a fraction of the cost of acquiring and maintaining physical servers and computers. This will enable them to concentrate on the development of their software with the cloud provider taking care of the technical installation and maintenance. Under this configuration, companies have the ability to manage software and services they develop, and the cloud provider manages physical devices. Cloud computing has numerous benefits compared to traditional computing including saving of cost and increase in flexibility. However, it also introduces security risks. Since data and applications are stored online, businesses must take measures to protect their information from threats like hacking and data breaches. In this paper, we will explore cloud computing, the key security risks involved, and the best practices for securing cloud services.

A. Traditional Computing

Traditional computing refers to a setup where businesses store and manage their own computers and software in physical data centers. These data centers are often constructed and nurtured by the business itself and connected by a network system that requires installation and management too [1]. As businesses develop these data centers to suit their requirements, they are able to institute the high level of security and customise

the configuration to suit their precise needs. This provides them with complete control of their infrastructure such as their configuration and maintenance. A business with direct control over their systems can guarantee the safety and confidentiality of their data and the services can be provided without the services of third parties. Moreover, in conventional computing, flexibility is high in upgrading or changing the computer system since all these are in-house [2]. However, while this level of control has its advantages, not every business can afford to build and maintain a physical data center. Setting up and running such an infrastructure requires significant investment in hardware, space, electricity, and IT personnel.

Another major challenge is scalability. If a business needs to handle more computing tasks or an increased number of users, it must add more servers and computers, which can be expensive and time-consuming. Concurrently, periods of times when more resources are required happen, which implies that the businesses might have an additional number of servers that are idle. This results in inefficiencies and wastages of finances. Even large companies have cases when their computer requirements may vary, it is not efficient to spend money on additional servers only to satisfy the temporary rise in demand. Cloud computing solves these challenges by offering a more flexible and cost-effective solution. Instead of building and managing their own data centers, businesses can use cloud services provided by third-party companies. These cloud providers manage the hardware and infrastructure, allowing businesses to access computing resources as needed.

B. Cloud Computing

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, businesses can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider [3]. Under cloud computing, the business is able to scale to high or low depending on the demand. In case they require additional servers during their peak times, they can just temporarily make use of the servers without necessarily having to buy and maintain additional hardware. Likewise, they are able to use it when there is a low demand and only pay as per their requirements. This renders cloud computing an viable and effective alternative of traditional computing, which allows businesses to save money and, at the same time, have the resources they require at any given time.

There is no big success that does not imply challenges, and cloud computing is not an exemption. It poses multiple threats including security and privacy risks like data breaches, unauthorized access, and compliance challenges to be seen as one of the most decisive. As the business data is placed in third party servers, the cloud provider and the business equally participate in ensuring that the data is secure. Good security alliances, including encryption and access control are needed. Incident Response (IR) and Disaster Recovery (DR) are two of the security risks that are critical in cloud computing. They also allow organizations to identify, contain and recover cybersecurity threats or system failure in their cloud environments faster, reducing downtime and data loss and ensuring business continuity. This is more so when it pertains to business, which has been depending on cloud infrastructure in carrying out key operations, since good IR and DR plans enable the business to bounce back to normalcy without causing a lot of effects in terms of operations and reputation.

C. Incident Response

Incident response, also known as cybersecurity incident response, is how an organization detects and reacts to cyber threats, or possible security breaches. It involves specific processes and technologies designed to identify and handle these threats effectively. A well-planned incident response strategy helps cybersecurity teams reduce or prevent damage from cyberattacks. The overall objectives are to prevent attacks and reduce their effects in case they occur, therefore cost reduction and decrease in business interruptions. Incident response is a major component of the general incident management that also involves business aspect of the situation like lawsuit, human resource and executive level decisions. To make sure that the process is systematic, entities develop an Incident Response Plan (IRP). This plan is a guide on how the various categories of cyber threats should be discovered, contained, and resolved. Having a strong incident response plan helps cybersecurity teams quickly detect and stop cyberattacks, restore affected systems, and reduce financial losses, legal penalties, and other negative consequences [4].

D. Disaster Recovery

Disaster recovery (DR) is a plan and process that helps an organization recover its systems, data, and operations after a major disruption, such as a cyberattack, natural disaster, or technical failure. The objective is to get regular business operations running within the shortest time possible and reduce time wastages and financial damages. A disaster recovery plan or DRP is the plan of action to follow in case of a disaster, such as data backup, system recovery, and other methods of even keeping business operations going. It provides the ability to recover essential systems and data in a short time would protect the effects on workforce, clients and business operations.

Business continuity is a necessary component of disaster recovery and aims at ensuring that the organization moves on even in unforeseen circumstances. Cybersecurity incident response is focused on cyber threats, whereas disaster recovery is more inclusive of disruptions, such as power disruption, equipment breakdowns, and disasters. Having a strong disaster recovery plan helps organizations avoid extended downtime, protect valuable data, and ensure a faster return to normal operations [5].

II. COMPARING INCIDENT RESPONSE AND DISASTER RECOVERY: TRADITIONAL VS. CLOUD APPROACHES

Incident Response (IR) and Disaster Recovery (DR) are critical strategies for handling cyber threats and system failures. While both aim to minimize damage and restore operations, their implementation varies depending on whether an organization uses traditional on-premises infrastructure or cloud-based services.

A. Understanding Incident Response (IR) in Traditional vs. Cloud

Incident Response (IR) is the process of detecting, investigating, and responding to cyber threats like malware, hacking, or data breaches. The key difference between traditional and cloud-based IR lies in how threats are detected, managed, and mitigated.

a. Traditional IR

- Firewalls, antivirus software and in-house monitoring tools are among the tools that security teams use to identify threats.
- Responses to incidents involve manual intervention, where IT teams investigate logs, isolate affected systems, and apply fixes.
- Limited scalability is also a possibility as security is limited to physical infrastructure of the organization.

Example: A firm has its own data center to which a phishing attack is introduced into and malware is placed on local servers. The IT staff service personnel detects infected systems by hand, deletes malware, and recovers files that were affected by malware by means of backups.

b. Cloud-Based IR

- Cloud service providers (AWS, Google Cloud, Azure) offer automated threat detection tools like real-time alerts, AI-driven security monitoring, and centralized logging.
- Automation and scalability of security responses can also be handled easily to deal with numerous threats at a time.
- There are security measures embedded within the cloud providers, automation of DDoS protection, and network isolation.

Example: A company using cloud-hosted applications faces a hacking attempt. The cloud provider's security system detects suspicious activity, blocks the attacker's IP, and notifies the IT team in real time.

B. Understanding Disaster Recovery (DR) in Traditional vs. Cloud

Disaster Recovery (DR), also known as the recovery of systems and data, involves the process when the system, data, or hardware unexpectedly fails, is subjected to attacks, or in the case of natural disaster recovery. The conventional and cloud computing methods vary in terms of speed, automation and infrastructure demands.

a. Traditional DR

- Businesses store backups on physical servers, external drives, or offsite data centers.
- Recovery is not automated and in most cases, IT personnel have to restore systems and this may take hours or even days.
- Hardware failure or loss of data may occur without updating or securing the backups, which is dangerous.

Example: A company's on-premises server crashes due to a power outage. IT staff must physically restart the server and restore files from backup disks, leading to several hours of downtime.

b. Cloud-Based DR

- Data is automatically backed up across multiple cloud locations.
- Recovery can be automated and immediate and can bring down the downtime to minutes as opposed to hours or days.
- Cloud services offer failover services, where the failure of one server by another one will take its place and there will be no disconnection of the service.

Example: A business that stores data on clouds is attacked by ransomware. They no longer have to pay a ransom but instead a few minutes later, their systems have been restored using the latest cloud backup.

C. Key Differences: Traditional vs. Cloud IR & DR

Both Incident Response (IR) and Disaster Recovery (DR) are essential for protecting an organization from cyber threats and unexpected disruptions. However, conventional on-premise solutions take much manual work and infrastructure and cost more and take a longer time to recover. Table-1 summarizes the key differences between traditional and cloud-based IR and DR approaches.

Table 1. Comparison of Traditional vs. Cloud-Based IR & DR

Feature	Traditional IR & DR	Cloud-Based IR & DR
Threat Detection	Manual, using local security tools	Automated, using AI-driven cloud security
Response Speed	Slower, requires IT staff intervention	Faster, often automated
Disaster Recovery Time	Hours or days	Minutes or seconds
Data Backup	Physical storage (servers, disks)	Cloud-based, across multiple locations
Scalability	Limited, requires more hardware	High, with automatic scaling
Cost	Expensive (hardware, IT staff)	Cost-effective (pay-as-you-go cloud services)

In contrast, cloud-based solutions offer automation, scalability, and faster recovery, making them a more efficient and cost-effective choice for modern businesses. It is worth mentioning though that cloud-based recovery is not fully automated. Management of the business and the cloud provider should collaborate to overcome challenges since issues of security and recovery are joint. Just relocated to the cloud does not imply that everything automatically becomes under control organizations still need to actively participate in the security and maintenance of their systems [6-9].

III. CORE PRINCIPLES AND BEST PRACTICES FOR INCIDENT RESPONSE IN CLOUD COMPUTING

Core principles serve as the foundation for an organization's decisions and actions, ensuring consistency, security, and efficiency in operations. Best practices, however, are established practices that can assist organizations to attain their objectives as well as conform to these fundamental principles. The combination of

these two creates a systematic way of addressing the incident response in cloud computing. A well-defined set of core principles significantly reduces security incidents, minimizes business disruptions, and prevents data loss. Additionally, it ensures compliance with regulatory requirements and enhances the organization's ability to adapt to evolving cloud infrastructure and emerging threats. In this part, we shall examine the key fundamental principles and best practices that companies should consider in enhancing their cloud infrastructure and enhancing incident response capabilities.

A. Core Principals

There are six key principles in incident response for cloud computing. Organizations should follow a structured approach that ensures all these principles are met for effective incident management.

1. **Preparation**: The initial principle is that one should be prepared even before an incident hits. This includes installing surveillance facilities, defining responsibilities and making response plans in case an incident occurs. The response plans also need to be regularly revised and enhanced to allow organizations to effectively respond to an incident promptly.
2. **Detection and Analysis**: This principle is aimed at devising automated systems and identifying abnormal activity, and analyzing the incident and identifying the underlying root cause of the incident prior to its escalation and resulting significant damage.
3. **Containment**: When a threat has been identified, it should be contained in order to limit the damage. This will include isolating the systems that are affected where possible, preventing traffic that is malicious and taking the procedures listed in the incident response plan to prevent the spread of an attack.
4. **Eradication**: After containment, organizations must eliminate the root cause of the incident. This step ensures that no traces of the attack remain, thereby reducing the risk of recurrence.
5. **Recovery**: This principle guarantees that systems and services are brought back to the normal operation without compromising the security. It is devoted to the minimization of the downtime and the check of the correct functioning.
6. **Post-Mortem**: After resolving the incident, organizations should analyze what happened, what worked, what did not work, and what needs improvement. The lessons learned should be recorded and passed around to enhance future response measures to incidents. This should be approached by involving people with different backgrounds and update the incident response plan.

By following these principles, organizations can enhance their ability to handle security incidents effectively and reduce risks in a cloud environment.

B. Best Practices

To effectively manage and mitigate security incidents in a cloud environment, organizations should follow these best practices:

1. **Establish a Clear Incident Response Plan**: Develop a well documented and planned incident response plan designed to be used in a cloud environment. Make sure that every stakeholder knows his or her roles and responsibilities.
2. **Automate Detection and Monitoring**: Use automated security tools and AI-based monitoring systems should be used to find threats at an early stage and minimize the response time.
3. **Enable Real-Time Logging and Analysis**: Logging and analyzing logs generated by cloud services continuously would help to detect any anomalies and possible security breaches in a short period of time.
4. **Implement Strong Access Controls**: Use Multi-factor authentication (MFA), least privilege and role-based access control (RBAC) can be used to restrict access to sensitive information and systems.
5. **Ensure Rapid Containment Measures**: Have a set of steps to isolate systems compromised, block malicious traffic and inhibit attacks.
6. **Use Cloud-Native Security Tools:** Leverage cloud service providers (CSPs) including AWS Guard Duty, Azure Security Center or Google Security Command Center to provide a better detection and response to threats.

7. **Regularly Test and Update Response Plans**: Run an incident response drill, penetration test, and tabletop to confirm that the plan is still valid and up to date.
8. **Implement Secure Backup and Recovery Strategies**: Maintain encrypted, regular back-ups of important data and conduct recovery tests in order to reduce the amount of time spent battling an incident.
9. **Coordinate with Cloud Providers**: Learn about shared responsibility model and build a strong communication with cloud providers to request them to take action regarding an incident.
10. **Conduct Post-Incident Reviews**: This is done post-mortem after every incident to determine lessons learned, better response plans, and revise policies based on these lessons.

By following these best practices, organizations can enhance their resilience against cyber threats and ensure a swift, effective response to security incidents in cloud environments [11-12].

IV. CORE PRINCIPLES AND BEST PRACTICES FOR DISASTER RECOVERY IN CLOUD COMPUTING

Disaster Recovery (DR) in cloud computing is a strategic approach to ensuring business continuity in the event of system failures, cyberattacks, or natural disasters. Currently, in contrast to the previous on-premise recovery approach, a cloud-based DR utilizes automation, scalability, and distributed resources to mitigate critical systems within a short time and reduce downtime. The presence of a well-designed Disaster recovery plan implies the ability of organizations to retrieve data and restore their operations effectively with the minimum inconvenience.

A. Core Principles of Cloud Disaster Recovery

1. **Data Replication and Backup**: Redundancy and replication comprise important aspects of a multi-cloud disaster recovery plan. They assist them in maintaining your data and apps on the move even when there are setbacks.
2. **Geographical Diversity**: Geographical diversity is one of the critical components of multi-cloud disaster recovery. It involves resources of storing your data and systems in non-single cloud providers in various locations. This assists in ensuring that your business does not stall down in case something goes wrong in one aspect.
3. **Automated Failover and Recovery**: Automated failover and recovery are key parts of a multi-cloud disaster recovery plan. They help keep your important apps and data working, even when problems happen.
4. Clear RTO and RPO: Clearly define and document your Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to ensure that your disaster recovery strategy aligns with business continuity goals
5. **Compliance and Security**: It is highly important to have your multi-cloud disaster recovery plan secure and to adhere to the rules.
6. **Regular Testing and Validation**: Testing and checking your multi-cloud disaster recovery plan frequently. This assists in ensuring that your plan performs well at the right time.

B. Best Practices for Disaster Recovery in Cloud Computing

To ensure business continuity and minimize downtime during a disaster, organizations should follow these best practices for disaster recovery (DR) in cloud environments:

1. **Develop a Comprehensive Disaster Recovery Plan**: Decide on Consistent Disaster Recovery Time Objective (RTO) (maximum downtime) and Recovery Point Objective (RPO) (maximum data loss) based on the needs of the business.
2. **Define Recovery Objectives**: Determine a Recovery Time Objective (RTO) (maximum allowable downtime) and Recovery Point Objective (RPO) (maximum allowable data loss) according to business requirements.
3. **Leverage Cloud-Based DR Solutions**: Automated failover and recovery in the use of cloud-native disaster recovery solutions, such as AWS Disaster Recovery, Azure Site Recovery or Google Cloud

Backup and DR.

4. **Implement Automated Backups**: Schedule regular, encrypted backups of critical data, applications, and configurations, ensuring they are stored in geographically diverse locations.
5. **Use Multi-Region and Multi-Cloud Strategies**: Distribute workloads across multiple cloud regions or providers to enhance resilience and reduce the risk of total failure.
6. **Ensure Redundancy and High Availability**: Deploy redundancy systems, databases and infrastructure components to enable availability in case of an outage.
7. **Test and Update the DR Plan Regularly**: Conduct regular disaster recovery drills, simulations, and tabletop exercises to verify effectiveness and identify gaps.
8. **Monitor and Automate Failover Mechanisms**: Introduce automated monitoring and failover systems to monitor and switch out to back up systems automatically.
9. **Secure DR Processes and Data**: Backup data should be strongly encrypted, controlled via access controls, and be abided by security standards to ensure unauthorized access and corruption.
10. **Establish Clear Communication and Documentation**: Maintain date documentation of the DR procedures and make the stakeholders aware of their role in the implementation of recovery plans.

By applying these principles and best practices, businesses can significantly enhance their disaster recovery capabilities in the cloud. To recover disruptions through cloud-based DR solutions is an easier, more resilient, and less expensive approach that will have a minimal effect on operations and customer experience [13].

V. CASE STUDY: THE CAPITAL ONE DATA BREACH - CHALLENGES IN CLOUD SECURITY INCIDENT RESPONSE AND RECOVERY

In July 2019, Capital One, a major financial institution, suffered a data breach that exposed the sensitive information of over 100 million individuals in the United States and Canada. This incident highlights the challenges organizations face in responding to cloud security breaches and recovering from their impact.

A. Incident Overview

In July 2019, Capital One, a large financial company, experienced a major data breach caused by a weakness in their cloud setup, which allowed a hacker to access and download sensitive data stored in the cloud. The hacker had circumvented the security by using a poorly configured firewall to access valuable files that had names, addresses, credit scores, Social Security numbers and bank account numbers. The breach went unnoticed for several months until someone discovered the leaked data online and reported it to Capital One. This case highlights the importance of properly configuring cloud systems, continuously monitoring them, and responding quickly to any issues.

B. Challenges in Incident Response

The breach exposed several gaps in Capital One's cloud security incident response, including:

1. **Cloud Environment Complexity**: Capital One's use of cloud infrastructure introduced complexities in managing cloud-specific vulnerabilities. The attacker exploited a misconfigured Web Application Firewall (WAF) through a Server-Side Request Forgery (SSRF) attack, gaining access to sensitive data. This highlights the difficulty of securing cloud environments and the need for robust configuration management.
2. **Shared Responsibility Model Misunderstanding**: Cloud security relies on a shared responsibility model between the cloud provider and the customer. In this case, Capital One was responsible for securing its data within the cloud, including proper configuration and access controls. Misinterpretations or gaps in fulfilling these responsibilities can result in serious vulnerabilities, as demonstrated in the breach.
3. **Identity and Access Management (IAM) Challenges**: The attacker took advantage of security settings that gave too much access to certain accounts. This allowed them to move around inside the system more than they should have been able to. It reveals a failure to enforce the principle of least privilege, which requires that users and services have only the minimum necessary access. Ongoing audits and strict IAM policies are essential to reduce these risks.

4. **Incident Detection and Response Delays**: Although the breach occurred in March 2019, it wasn't discovered until July 2019. This significant delay in detection and response illustrates the need for effective monitoring tools and rapid incident response capabilities to minimize the scope and damage of such attacks.

C. Challenges in Recovery

Recovering from the attack took a lot of time, effort, and money. Key challenges included:

1. **Financial Repercussions**: Capital One anticipated incurring costs between $100 million and $150 million in 2019 due to the breach. Such costs included customer alerts, credit services, technology upgrades, and legal assistance. The company was also fined by the Office of the Comptroller of the Currency 80m due to the failure to comply with risk management and information security practices.
2. **Legal and Regulatory Scrutiny**: The breach led to multiple lawsuits, including class-action suits alleging negligence in protecting customer data. Transparent communication, quick remediation, and strong customer support were crucial in restoring confidence.
3. **Rebuilding Customer Trust**: Millions of customers were affected, raising concerns about Capital One's ability to protect sensitive information. Transparent communication, quick remediation, and strong customer support were crucial in restoring confidence.
4. **Operational Disruption**: The incident required a significant number of resources in terms of investigation, remediation, and communication, which could come at the cost of daily business activities and strategies.

The solution to these problems is a complex and active security strategy, the presence of a clear vision of the responsibilities of cloud security, effective IAM management, constant monitoring, and a culture of cybersecurity at all organizational levels.

D. Lessons Learned

Here are some lessons organizations can learn from this incident:

- **Clarify Shared Responsibility**: The misunderstanding of shared responsibility model between the providers and the customers of the cloud service could lead to serious security defects. It is important to define clearly and know the respective security duties of each party.
- Encrypt Sensitive Data: Use effective encryption methods to secure sensitive data during transit and at rest which will help reduce the data compromise risk.
- **Enforce the Principle of Least Privilege**: Any access to sensitive data or systems must be granted under a need to know basis, and there is therefore a narrowing of the possible attack surface.
- **Conduct Regular Security Testing**: Routine vulnerability assessments, penetration testing, and security simulations should be conducted to proactively identify and address security weaknesses before they can be exploited by adversaries.
- **Ensure Operational Resilience**: Cybersecurity incidents can severely disrupt business operations. Thus, security planning should establish detailed technologies of disaster recovery and business continuity to ensure resilience of operations.
- **Regularly Review Cloud Configurations**: Continuous assessment of cloud environment configurations is critical. By using automated tools, the process of misconfigurations that can bring risk can be identified and fixed.

The data breach at Capital One should be used as a lesson to show how complex the process of managing and recovering after cloud security breaches is to consumers. It emphasizes the critical need for proactive security measures, continuous monitoring, and a clear grasp of shared responsibilities to safeguard sensitive data in the cloud [14-17].

VI. EMERGING TRENDS IN THREAT DETECTION AND AUTOMATED DISASTER RECOVERY

Artificial Intelligence (AI) has been revolutionary to the cybersecurity technology and disaster recovery, making organizations more dependable and resilient. Artificial intelligence systems are leading the pack in

automated threat detection and recovery in case of disaster, strengthening against new technology threats and providing business continuity.

A. AI-Implemented Threat Detection

Detecting cyber threats is getting harder because attacks are becoming more advanced and frequent. AI makes this easier by automating the process and spotting unusual behavior in real time. Here's how:

- **Anomaly Detection (Finding Unusual Activity**): AI systems can be used to analyze network data in order to create a baseline behavior. Any of these norms could be deviated, which is a sign of the possible threat, and it is possible to take prompt measures to stop the situation. As an example, AI is able to tell when a user is accessing data in an abnormal manner such as a user downloading a lot of data which can be a sign of a security breach.
- **Behavioral Analytics**: AI is able to detect insider threats based on the activity of a user even with limited data. Indicatively, when a user with an account in the system accesses highly confidential materials at odd times, AI can alert of such actions to be pursued.
- **Automated Response**: AI systems do not only identify threats but also perform immediate countermeasures, i.e. isolate compromised systems or block malicious IP addresses. Reduction in response time is an important benefit of AI-based security.

The usefulness of AI in detecting threats is visible in the industrial use. As an example, Palo Alto Networks has raised its forecasts on the annual revenues because of the rise of the demand on AI-augmented cybersecurity services. This growth was credited by the company CEO to the use of AI technologies, more spending on clouds, and improvement of infrastructure [18-19].

B. Disaster Recovery Automation

Rapid recovery from disruptions is critical for maintaining business operations. Automated disaster recovery uses AI and machine learning to improve the efficiency and reliability of recovery. Key features include:

- **Automated Failover**: AI systems can autonomously redirect operations to backup systems or alternative data centers, minimizing downtime without human intervention.
- **Predictive Analytics**: AI forecasts potential system failures using performance data, allowing organizations to take preemptive action and avoid unexpected shutdowns.
- **Consistent Recovery Processes**: Automation will remove the human error, which guarantees the strict compliance with the recovery procedures and the impeccable implementation of disaster recovery procedures.

Companies like Zerto have come up with a solution that is used to automate disaster recovery in different ecosystems including the public clouds. With their platforms, several virtual machines can be secured, and operations will be continued with minimal human involvement [20-21].

VII. CONCLUSION

The move to cloud computing has brought major changes to how businesses manage IT services and security. It offers significant advantages such as flexibility, lower costs, and the ability to scale quickly, but it also introduces new challenges particularly in the areas of incident response and disaster recovery. The benefits of it include flexibility, reduced cost, and scalability within a short time, but it also presents new challenges especially when it comes to incident response and disaster recovery. These activities which previously were handled fully within the systems of a company now involve close cooperation with cloud service providers. Consequently, the organizations should have a clear definition of which duties are under their responsibility and those that are being taken by the provider.

These changes make it even more significant that businesses should be equipped with properly worked-out strategies aimed at working in clouds. The experience of security breaches in the real world has demonstrated how harmful the absence of a clear, cloud-specific plan may be. Meanwhile, emerging technologies, such as automation and AI, start to allow more rapid detection, more precise response, and more effective recovery of operations, than never before. With the adoption of cloud increasing, companies must be keen on approaching

cloud security infrastructures with strong and flexible frameworks. This does not only involve the proper utilization of the appropriate tools but also the establishment of effective communication and coordination among the teams and cloud providers within the organization. Being proactive, adopting latest technologies, and adhering to established security procedures, companies can significantly enhance their resilience to cyber threats and detrimental impacts following such disruption that would help maintain long-term stability and success in the ever-digitized world.

Conflicts of Interest Statement

The author declares that there are no conflicts of interest.

Funding Statement

No funding was received for this study.

VIII. REFERENCES

1. TutorialsPoint, Difference Between Cloud Computing and Traditional Computing, TutorialsPoint, Online: https://www.tutorialspoint.com/difference-between-cloud-computing-and-traditional-computing
2. PennComp IT Services, Cloud Computing vs Traditional Computing, PennComp, Online: https://penncomp.com/cloud-computing-vs-traditional-computing/
3. Amazon Web Services, What Is Cloud Computing?, Amazon Web Services, Online: https://aws.amazon.com/what-is-cloud-computing/
4. IBM, Incident Response, IBM, Online: http://ibm.com/think/topics/incident-response
5. Cutover, Step-by-Step Guide: Create a Cybersecurity Disaster Recovery Plan, Cutover, 2022, Online: https://www.cutover.com/blog/step-by-step-guide-create-cyber-security-disaster-recovery-plan
6. N2WS, Disaster Recovery in the Cloud: Pros, Cons, and Choosing a Solution, N2WS, Online: https://n2ws.com/blog/disaster-recovery-in-the-cloud-pros-cons-and-choosing-a-solution#vs
7. TierPoint, Disaster Recovery: Cloud vs On-Premise, TierPoint, 2023, Online: https://www.tierpoint.com/blog/disaster-recovery-cloud-vs-on-premise/
8. Aztech IT Solutions, Cloud Computing vs Traditional, Aztech IT Solutions, Online: https://www.aztechit.co.uk/blog/cloud-computing-vs-traditional
9. Mitiga, Why Traditional Incident Response Doesn't Work in the Cloud, Mitiga, 2022, Online: https://www.mitiga.io/blog/why-traditional-incident-response-doesnt-work-cloud
10. DataGuard, What Are the Principles of Incident Response?, DataGuard, Online: https://www.dataguard.com/blog/what-are-the-principles-of-incident-response/
11. Sprinto, Cloud Incident Response, Sprinto, 2023, Online: https://sprinto.com/blog/cloud-incident-response/
12. Dig8ital, Cloud Incident Response, Dig8ital, Online: https://dig8ital.com/post/cloud-incident-response/
13. Coherence, Multi-Cloud Disaster Recovery: 5 Key Principles, Coherence, Online: https://www.withcoherence.com/articles/multi-cloud-disaster-recovery-5-key-principles
14. Shaharyar Khan et al., "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned," *ACM Transactions on Privacy and Security*, pp. 1-29, no.3, 2023. Google Scholar | Publisher Link
15. N. Novaes Neto et al., "A Case Study of the Capital One Data Breach," *SSRN Electronic Journal*, 2020. Google Scholar | Publisher Link
16. Dark Reading, Capital One Breach Conviction Exposes Scale of Cloud Entitlement Risk, Dark Reading, 2022, Online: https://www.darkreading.com/cloud-security/capital-one-breach-conviction-exposes-scale-of-cloud-entitlement-risk
17. AppSecEngineer, AWS Shared Responsibility Model: Capital One Breach Case Study, AppSecEngineer, 2023, Online: https://www.appsecengineer.com/blog/aws-shared-responsibility-model-capital-one-breach-case-study
18. Amazon Web Services, Automating Database Disaster Recovery, AWS Prescriptive Guidance, Online: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-database-disaster-recovery/automating.html
19. Palo Alto Networks, AI in Threat Detection, Palo Alto Networks, Online: https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection
20. BigID, AI Threat Intelligence, BigID, 2023, Online: https://bigid.com/blog/ai-threat-intelligence
21. Fortinet, Artificial Intelligence in Cybersecurity, Fortinet, Online: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity