Cloud Technologies and Critical Infrastructure Security: A Literature Review

April 2025

1 Introduction

Critical infrastructures are what today's society is made of. Countries rely on these systems to provide their populations with essentials such as energy, water, and food. To ensure that these resources are properly distributed, governments have increasingly used technology to meet growing population demands. Any issue with these critical infrastructures, such as power outages, cyberattacks, or supply chain failures, can have disastrous effects on public safety, national security, and economic stability. As a result, protecting these resources becomes a primary concern, increasing the need for an efficient, scalable, and most importantly secure solution.

Cloud technologies improve security through the use of data-driven decision making (Ambasht, 2023), AI-powered monitoring (Joyce, 2024), and real-time threat detection (Palo Alto Networks, n.d.). These solutions also positively contribute to critical infrastructures due to their ability to increase efficiency, reduce costs, and improve resilience (Joyce, 2024). However, this introduces threats specific to the cloud, such as hyperjacking (Department of Homeland Security, 2017), while still being susceptible to the usual threats, such as supply chain attacks. Furthermore, questions regarding accountability also become more complicated in a cloud environment.

This literature review aims to critique the use of cloud technologies in critical infrastructure and evaluate how it benefits critical infrastructure security, while also addressing the threats they pose and possible mitigations against them. I will attempt to answer these two questions:

1. How can cloud technologies improve critical infrastructure security?
2. What are the security challenges of migrating to the cloud and how can they be mitigated?

According to the National Institute of Standards and Technology (NIST, 2016), critical infrastructures are "the essential services that support a society and serve as the backbone of the society's economy, security and health". In the past, the UK had relied mainly on on-premise IT infrastructure, which is physically located in company facilities, consisting of servers, storage devices, and networking equipment (EG Innovations, n.d.). However, with the increasing demand for efficiency and security, the UK has begun to migrate to cloud infrastructure for its critical systems.

To help streamline this process, the Crown Commercial service created the G-Cloud framework, "a digital marketplace that simplifies procurement processes for public sector organisations in the UK. With G-Cloud 14, public sector bodies can now easily access pre-approved suppliers to meet their digital transformation needs, with solutions ranging from cloud software and hosting to security and compliance" (Hayes, 2024). "From 2012/13 to 2023/24, total government G-Cloud spend, which includes spending across multiple entities, including charities, was £17.3 billion." (Horton, 2024) This has led to easier adoption of the cloud and its services in a variety of sectors.

2 Benefits of Using the Cloud for Critical Infrastructure Security

There is a variety of literature that supports the role of cloud computing in improving critical infrastructure security. Cloud service providers (CSPs) offer a variety of security tools that help enhance protection, reducing the workload compared to manually securing environments.

It is especially important for services like energy grids, healthcare and emergency services to operate without any disruption. Here, the need to have continuous monitoring for threats is essential. CSPs address this issue by providing tools that give real-time visibility into system activity. Solutions like context-aware policy controls help enforce and remediate violations to detect suspicious behaviour. In addition, real-time threat intelligence

aids in detecting and preventing new malware (Palo Alto Networks, n.d.). Having tools like these ensure that data loss and downtime are kept to a minimum, both necessary in critical infrastructure.

van Niekerk and Jacobs (2013) highlight that the services that come from cloud solutions provide a positive effect for Critical Information Infrastructure Protection (CIIP). A notable example they use is elasticity, which is the ability to scale resources and security. Elasticity keeps environments protected during high traffic periods or Distributed Denial-of-Service (DDoS) attacks. Having specific dedicated services like AWS Shield for DDoS mitigation, high volume attacks can be better managed compared to on-premise models, allowing critical infrastructures to operate without disruption.

It is important to note that van Niekerk and Jacobs (2013) suggest that "cloud-based security solutions is not yet ready to be deployed as the only security measure". This is due to the current limitations of cloud-based security. For example, they mention cloud-based tools have problems with encrypted traffic, do not provide sufficient defence against insider threats, and rely heavily on standardised service models that may not align with the requirements for critical infrastructure. To be more secure, they suggest employing a layered or hybrid security model, which would combine the advantages of the cloud with traditional defences from on-premise models.

3 Security Threats in the cloud environment

While cloud computing offers many advantages, it also introduces a range of unique risks, which would have detrimental effects on critical infrastructure if not addressed properly. Cloud models are susceptible to insider threats, misconfiguration errors, and unclear delegated responsibility between CSPs and users.

A report from SentinelOne (2024) states "Almost 23% of cloud security incidents are a result of cloud misconfiguration", making misconfigurations one of the most common and harmful threats in cloud environments. An example can be seen in the 2019 Capital One data breach, where data from more than 100 million customers were leaked. This breach was caused by a former AWS employee exploiting a misconfigured Web Application Firewall (WAF), allowing him to perform a Server-Side Request Forgery (SSRF) attack (Khan et al., 2022). Although the AWS infrastructure was not compromised, a large-scale attack exposing customer data still occurred, demonstrating the result of malicious insiders and cloud misconfigurations.

After this incident, the shared responsibility model was critiqued. Khan et al. (2022) analysed Capital One's cybersecurity structure and identified weak technical safeguarding and management oversight as a key point of failure. This is supported by the Cert-EU (2019) incident summary, which states "The breach purportedly exploited a misconfigured web application used to access the cloud infrastructure". Wagner et al. (2015) suggests conducting service-specific risk assessments to support informed decision-making. This may have identified the misconfigurations and access control flaws before the attack took place.

These types of security failures give rise to a broader issue regarding accountability in cloud systems. Younis, Merabti and Kifayat (2013) raise broader concerns about cloud environments, highlighting the importance of having robust access control, auditing, and policy enforcement. Similarly, Mackay, Baker, and Al-Yasiri (2012) also highlighted the lack of trust in cloud platforms.

CSPs provide governance tools, like AWS GuardDuty, as a protective measure to help continuously monitor and detect misconfigurations (CloudOptimo, 2025). These tools increase visibility into the platform through real-time threat detection and alerts when misconfigurations occur. However, these solutions may not be able to be properly implemented due to inadequate investment into security (ISC2, 2023), making it harder for staff to use these tools to their full potential.

Another example is the Colonial Pipeline ransomware attack in 2021. Here, on-premises IT systems were targeted, but the attack still highlights weaknesses in remote access and authentication systems (imprivata, 2022), key components of the cloud security architecture. Adversaries were able to take advantage of reusing credentials and the lack of multi-factor authentication (MFA) to breach the system and stop fuel distribution across the US East Coast (Bellamkonda, 2024). Stratodesk (2021) reflects on these attacks and states how it could have been mitigated if they simply used MFA. These examples show that migration to the cloud does not protect against security vulnerabilities, but shifts where they might be. As previously mentioned, van Niekerk and Jacob (2013) suggested that cloud-based security should not be a direct replacement, but instead compliment them in a layered hybrid security model. An example here could be to combine the elasticity of the cloud with the control of an on-premise model, which would increase resiliency for critical infrastructures.

4 Mitigation strategies

Organisations have created specific security strategies to counteract the challenges of cloud threats. Some of the most notable are Zero Trust Architecture (ZTA), Cloud Security Posture Management (CSPM), and policy-driven governance frameworks.

According to NIST (2020), a zero trust architecture (ZTA) is an enterprise cybersecurity architecture based on zero trust principles designed to prevent data breaches and limit internal lateral movement. A perimeter-based model trusts users within an organisation, but ZTA assumes breach, requires explicit verification, and enforces least privilege access. These strategies are particularly useful in cloud environments, where it is common for multiple users to access resources remotely from different devices. These solutions are present in cloud environments, but there are challenges in implementing them in legacy systems, where authentication systems and outdated architecture complicate the adoption of ZTA (Tackley, 2024). This may be a challenge for critical infrastructure organisations that have not yet migrated to the cloud.

CSPM tools provided by CSPs, such as AWS Config and Microsoft Defender, detect misconfigurations in cloud environments and enforce compliance, improving the security posture. Microsoft (n.d.) states that the CSPM tools are effective for technical control and help mitigate against misconfiguration, a primary cause of cloud breaches. These tools help organisations audit their environments, detect policy violations, and remediate them before adversaries can exploit them.

In terms of governance frameworks, van Niekerk and Jacobs (2013) suggest using a layered security model that includes policy and technical enforcement, especially for critical infrastructure security. They highlight that the cloud should not be the only security solution, but instead should be part of a hybrid model. Wagner et al. (2015) suggest conducting service-specific risk assessments to support informed decision-making, indicating that CSPM tools may not be effective against certain specific vulnerabilities depending on the CSP.

In addition, both Mackay, Baker, and Al-Yasiri (2012) and Younis, Merabti and Kifayat (2013) raise concerns about accountability not being specific enough. They argue that ambiguity over legal responsibilities can arise if Service Level Agreements (SLAs), a contract between a CSP and a customer that defines the expected level of service (Amazon Web Services), are not properly defined.

The literature seems to be both in support of utilising cloud services and cautious about it at the same time. Mitigations must not rely on the cloud itself, but use a model that incorporates the cloud with strategic planning in hybrid models.

5 Conclusion

The purpose of this literature review was to answer two key questions: How cloud technologies can improve critical infrastructure security and what security challenges come from their adoption. It is clear that the use of cloud computing has its advantages, including real-time threat detection, improved availability, and scalability. However, these advantages are undermined by its respective risks, such as misconfigurations, insider threats, and unclear accountability due to the shared responsibility model.

The literature strongly supports the idea that fully relying on the cloud as a replacement for existing security models is insufficient to protect environments, and a hybrid security model should be adopted instead, with layered models that use both safeguarding tools and layered governance. Tools such as ZTA and CSPM are effective in mitigating insider threats, but only when combined with process-driven migration strategies and clear SLAs. However, there are still concerns about the compatibility of legacy systems and operational oversight.

Although the literature generally agrees on core principles, scholars are separated when it comes to implementation. Future research should prioritise real-world case studies of hybrid cloud environments in critical infrastructure, studying long-term outcomes, and if enforcing SLAs, correct configurations, and regulatory frameworks work better than it is now. There should be more focus on the impacts of cloud computing in specific critical sectors, such as water or finance, the threats relating to those individual sectors, and how cloud model could mitigate against them.

References

Ambasht, A., 2023. *Real-time data integration and analytics: Empowering data-driven decision making.* International Journal of Computer Trends and Technology. [Online] Available at: https://www.researchgate.net/publication/372521979_Real-Time_Data_Integration_and_Analytics_Empowering_Data-Driven_Decision_Making [Accessed 2 Apr. 2025].

Amazon Web Services, n.d. *What is a Service Level Agreement (SLA)?*. Amazon Web Services. [Online] Available at: https://aws.amazon.com/what-is/service-level-agreement/ [Accessed 3 Apr. 2025].

Barker, E. and Barker, W.C., 2016. *Guideline for using cryptographic standards in the federal government: Directives, Mandates and Policies*. Gaithersburg: National Institute of Standards and Technology. [Online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175A.pdf [Accessed 2 Apr. 2025].

Bellamkonda, S., 2024. *Ransomware attacks on critical infrastructure: A study of the Colonial Pipeline incident*. IAEME. [Online] Available at: https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_7_ISSUE_2/IJRCAIT_07_02_110.pdf [Accessed 2 Apr. 2025].

CERT-EU, 2019. *Massive breach at Capital One, purportedly due to a cloud misconfiguration*. CERT-EU. [Online] Available at: https://cert.europa.eu/publications/threat-intelligence/threat-memo-190802-1/pdf [Accessed 2 Apr. 2025].

Department of Homeland Security, 2017. *Risks to Critical Infrastructure that use Cloud Services*. Department of Homeland Security. [Online] Available at: https://info.publicintelligence.net/DHS-OCIA-InfrastructureCloudRisks.pdf [Accessed 2 Apr. 2025].

Easterly, J. and Fanning, T., 2023. *The Attack on Colonial Pipeline: What We've Learned and What We've Done Over the Past Two Years*. CISA. [Online] Available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years [Accessed 2 Apr. 2025].

EG Innovations, n.d. *What is On-premises*. EG Innovations. [Online] Available at: https://www.eginnovations.com/glossary/on-premises [Accessed 2 Apr. 2025].

Hayes, D., 2024. *G-Cloud 14 is Live: GlobalSign Empowers the Public Sector with Enhanced Digital Security*. GlobalSign. [Online] Available at: https://www.globalsign.com/en/blog/g-cloud-14-live-globalsign-empowers-public-sector-enhanced-digital-security [Accessed 2 Apr. 2025].

Horton, C., 2024. *Public sector to waste £300 million on restrictive cloud licensing*. THINK Digital Partners. [Online] Available at: https://www.thinkdigitalpartners.com/news/2024/07/04/public-sector-to-waste-300-million-on-restrictive-cloud-licensing-report/ [Accessed 2 Apr. 2025].

Hu, V.C., Iorga, M., Bao, W., Li, A., Li, Q. and Gouglidis, A., 2021. *General Access Control Guidance for Cloud Systems*. Gaithersburg: National Institute of Standards and Technology. [Online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf [Accessed 2 Apr. 2025].

Imprivata, 2022. *The role of identity in digital transformation*. Imprivata. [Online] Available at: https://www.imprivata.com/uk/node/103640 [Accessed 2 Apr. 2025].

ISC2, 2023. *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce*. ISC2. [Online] Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e [Accessed 2 Apr. 2025].

Joyce, R., 2024. *How AI-powered cloud monitoring helps prevent downtime and data loss*. CloudMonitor. [Online] Available at: https://cloudmonitor.ai/2024/11/how-ai-powered-cloud-monitoring-helps-prevent-downtime-and-data-loss/ [Accessed 2 Apr. 2025].

Khan, S., Kabanov, I., Hua, Y. and Madnick, S., 2022. *A systematic analysis of the Capital One data breach: Critical lessons learned*. Association for Computing Machinery. [Online] Available at: https://dl.acm.org/doi/10.1145/3546068 [Accessed 2 Apr. 2025].

Krishnakumar, V., 2025. *AWS GuardDuty: Advanced Threat Detection for Cloud Security*. CloudOptimo. [Online] Available at: https://www.cloudoptimo.com/blog/aws-guardduty-advanced-threat-detection-for-cloud-security/ [Accessed 3 Apr. 2025].

MacKay, M., Baker, T. and Al-Yasiri, A., 2012. *Security-oriented cloud computing platform for critical infrastructures*. Computer Law and Security Review, 28(6), pp.679–686. doi:10.1016/j.clsr.2012.07.007. [Accessed 2 Apr. 2025].

Microsoft, n.d. *What is CSPM?*. Mircrosoft. [Online] Available at: https://www.microsoft.com/en-gb/security/business/security-101/what-is-cspm#layout-container-uid4f163 [Accessed 3 Apr. 2025].

Palo Alto Networks, n.d.a *Cloud threat detection*. Palo Alto Networks. [Online] Available at: https://www.paloaltonetworks.com/prisma/cloud/cloud-threat-detection [Accessed 2 Apr. 2025].

Palo Alto Networks, n.d.b *What is cloud security?*. Palo Alto Networks. [Online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-security? [Accessed 2 Apr. 2025].

Rose, S., Borchert, O. and Mitchell, S., 2020. *Zero Trust Architecture*. Gaithersburg: National Institute of Standards and Technology. [Online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [Accessed 2 Apr. 2025].

SentinelOne, 2024. *50+ Cloud Security Statistics in 2025*. SentinelOne. [Online] Available at: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/ [Accessed 3 Apr. 2025].

Smith, J. and Lee, A., 2022. *Privacy and security in cloud computing: Challenges and solutions*. Association for Computing Machinery. [Online] Available at: https://dl.acm.org/doi/10.1145/3546068 [Accessed 2 Apr. 2025].

Stratodesk, 2021. *Colonial Pipeline Cyber Attack Shows the Importance of Multi-Factor Authentication in 2021*. Stratodesk. [Online] Available at: https://www.stratodesk.com/colonial-pipeline-cyber-attack-shows-the-importance-of-multi-factor-authentication/ [Accessed 3 Apr. 2025].

Tackley, 2024. *What is Zero Trust Architecture and is it a Must in your Security?*. DataGuard. [Online] Available at: https://www.dataguard.com/blog/what-is-zero-trust-architecture-is-it-a-must-in-security/ [Accessed 3 Apr. 2025].

van Niekerk, B. and Jacobs, P., 2013. *Cloud-based security mechanisms for critical information infrastructure protection*. In: 2013 International Conference on Adaptive Science and Technology (ICAST). IEEE. doi:10.1109/ICASTech.2013.6707500. [Accessed 2 Apr. 2025].

Wagner, C., Hudic, A., Maksuti, S., Tauber, M. and Pallas, F., 2015. *Impact of Critical Infrastructure Requirements on Service Migration Guidelines to the Cloud*. In: 2015 3rd International Conference on Future Internet of Things and Cloud. IEEE, pp.1–8. doi:10.1109/FiCloud.2015.79. [Accessed 2 Apr. 2025].

Younis, A., Kifayat, K. and Merabti, M., 2013. *Secure cloud computing for critical infrastructure: A survey*. ResearchGate. [Online] Available at: https://www.researchgate.net/publication/262817790_Secure_Cloud_Computing_for_Critical_Infrastructure_A_Survey [Accessed 2 Apr. 2025].