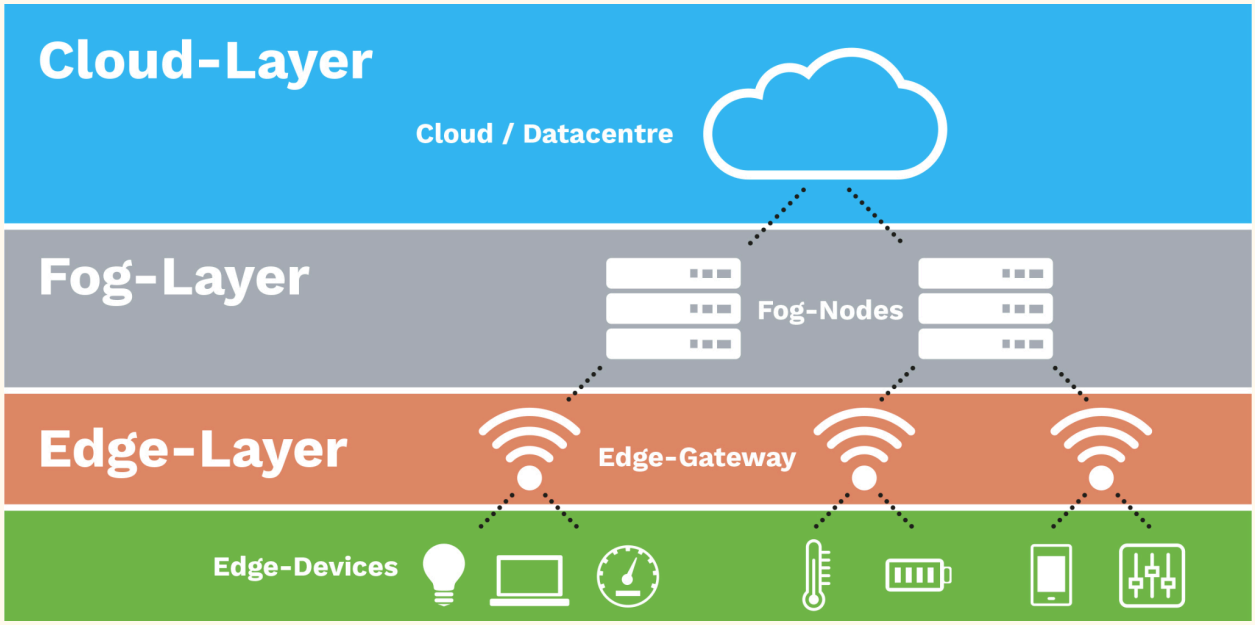
Prof in Forensics & Security

Investigating Cyber-Crime: Unravelling the Challenges in Cloud, Fog, and Edge Environments

—

By Luke Dawson (P2665421)



Introduction

In the modern day of computing and contemporary digital landscape, the introduction of cloud, fog, and edge computing paradigms that have been introduced revolutionise the way data is processed, stored, and accessed. However, this technological evolution has escalated the complexity and size of cyber-crime challenges. These computing environments, characterised by their distributed nature and vast processing capabilities, present a ground for various cybercriminal activities *(Kebande & Ray, 2020; Lillis et al., 2016)*. This essay aims to dissect the multiple challenges posed by cyber-crime within cloud, fog, and edge computing environments, shedding light on the technological and legal intricacies involved. When integrating insights from seminal studies and reports, such as those by *Alrawais et al. (2020)* and *Yi, Qin, and Li (2017)*, this essay aims to delineate the current cybersecurity landscape, highlight the imperative for robust defence mechanisms, and explore the alignment of technological outcomes with prevailing legal frameworks. Throughout this essay I will aim to provide a critical examination of the existing literature. This essay will navigate the intricate web of cyber-crime investigation challenges, with a particular focus on the implications for privacy, data integrity, and legal compliance in this new digital age.

Cloud Computing

Introduction to Cloud Computing

Cloud computing represents a pivotal shift in computing, allowing for a scalable, on-demand access to computing resources via the Internet. This model also allows for efficient data storage, application execution, and utilisation of processing capabilities without direct management of physical servers. This has become essential for enhancing operational efficiency and cost-effectiveness, which allows for users to constantly adjust resources based on their needs. This Cloud model supports a diverse array of services including data analytics, virtual storage, and software development, driving these technological advancements and transforming practices. This significance within the Uk's digital economy is highlighted by its adoption across public and private sectors, aligning with the nation's transformation strategies.

Challenges for Forensic Investigators in the Cloud

Within the world of forensic investigations, cloud computing, particularly within the context of the UK, are met with distinctive challenges. Data jurisdiction is one of the primary concerns, as cloud services often distribute data across various global locations. This application complicates legal authority, especially when data is stored outside of the UK, raising issues around international law and sovereignty *(Huntsman Security, 2022)*.

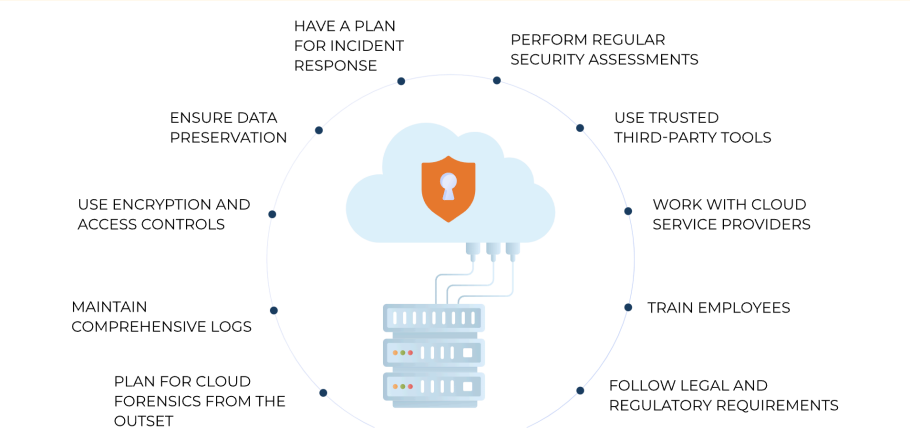


Figure 1: Cloud Security Strategy Diagram

Encryption, which is a critical element of data security within cloud environments, poses significant barriers to forensics investigations. Accessing encrypted data typically requires decryption keys, entailing legal processes or cooperation from service providers. The UK's Investigatory Powers Act 2016, highlights the complexities involved in balancing privacy concerns with investigatory needs.

Furthermore, the multi-tenancy[1] nature of cloud computing, where the infrastructure is shared among multiple users, introduces difficulties in isolating relevant data without compromising privacy. This forensic method is both effective and respectful towards the data protection laws, including the Data Protection Act 2018, which implements DDPR principles *(Information Commissioner's Office, 2018)*.

Legal and Regulatory Framework

The legal and regulatory landscape for cloud computing in the UK encompasses stringent data protection and privacy regulations. The Data Protection Act 2018 and GDPR provide detailed guidelines for data management and privacy, directly impacting forensic practices in cloud environments. Navigating this complex legal framework requires an understanding of both

domestic and international laws to effectively conduct forensic investigations within cloud computing environments. The evolving nature of UK law, alongside ongoing technological advancements, highlights the need for continuous legal adaptations and collaborations to address cybercrime effectively.

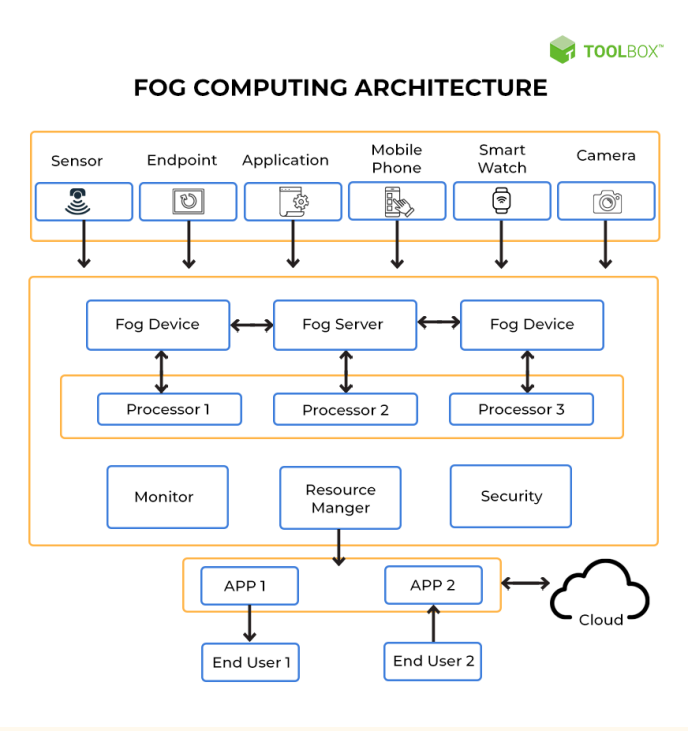
Fog Computing

Introduction to Fog Computing

Fog computing, which is an extension of cloud computing, takes computational resources closer to the data source, while enhancing efficiency and reducing latency during the data processing. By decentralising the data analysis and storage[2], fog computing allows for real-time applications, IoT (Internet of Things) devices, and mobile computing with greater agility. Fog computing aligns with various smart city projects and IoT structure, giving improvements to sectors like healthcare, transportations, and urban management. Its adoption highlights a move towards more responsive services.

Challenges for Forensic Investigators in the Fog

Figure 2: Fog Computing Architecture



Forensic investigations within fog computing environments often encounter challenges, which are then magnified by the distributed nature of Fogs architecture. As digital evidence plays a critical role within legal proceedings, the short-lived nature of data in fog nodes creates a complicated atmosphere during evidence preservation and retrieval. This is then compounded through the vast volume of data that is generated by IoT devices, making it more difficult when pinpointing the relevant information

without the use of forensic tools *(Zawoad et al., 2017)*.

Another significant challenge that Fog brings is Data origin; due to having to trace data lineage through multiple fog nodes in order to help establish its origin and integrity is essential during its process but it is daunting due to the lack of centralised control Fog provides. This aspect is crucial for allowing the standards to match what the courts ask for, as admissibility of digital evidence relies on demonstrable chain of custody and data integrity *(Casey, 2011)*.

Furthermore, the configuration of the environments can complicate the replication of digital crime scenes (a critical step in forensic analysis). This ensures that investigators must navigate these obstacles while cooperating with the UKs legal framework, including compliance with the *Investigatory Powers Act 2016*, which focuses on digital surveillance and data collection.

Legal and Regulatory Framework

Like the Cloud environment, Fog has a complex legal and regulatory framework created by the various laws and guidelines created by the UKs justice system, these aim to help balance technological advancement with privacy and security considerations. For example, the *Data Protection Act 2018*, helps embody the GDPR principles, that impose stringent requirements on data handling, which directly impacts forensic activities in Fog computing. Because of this investigators must ensure compliance with the regulations when engaging in their forensic practices, particularly in the handling of personal and sensitive data across distributed networks.

A common feature in fog computing is Cross-border data flow[3] this feature introduces additional legal challenges, as navigation through international laws and agreements is challenging, even more so now in a post-Brexit state. Due to the UKs' departure from the EU, creates a reevaluation of data transfer mechanisms to ensure that personal and sensitive data is continued to be protected and keeps legal compliance, highlighting the need for robust agreements and clarity in international cooperation for digital investigations *(Peers, 2020)*.

Edge Computing

Introduction to Edge Computing

Different to Cloud and Fog computing, Edge represents a paradigm shift[4], emphasising the data's processing at the network, due to its closer source of data generation. This technological

advance is crucial within countries, especially the UK, as it facilitates real-time analytics and decision-making in IoT applications. Edge has a unique scheme of utilising minimal latency and reduced bandwidth consumption as it helps align with the strategic digital initiatives that come with investigations aiming to increase efficiency and innovation. It also embodies the commitment to harness cutting-edge technologies, allowing for the UK to remain as one of the forefront in the digital economy's evolution.

Challenges for Forensic Investigators in the Edge

Similarly to both Cloud and Fog, Edge computing does come with challenges for forensic investigators, within the UK these challenges are primarily due to the decentralisation of the data being processed and stored. The nature of the data in Edge computing complicates traditional forensic methodologies designed for more centralised systems. As *Berry (2010)* notes, the forensic community must adapt to these evolving computing environments, creating new techniques in evidence collection and analysis in order to contend with the increasing volume, velocity, and variety of the data that is being generated. Furthermore, the intricate legal landscape, including the *Investigatory Powers Act 2016*, states that meticulous adherence to lawful gathering, ensures that investigative actions are defensible in court.

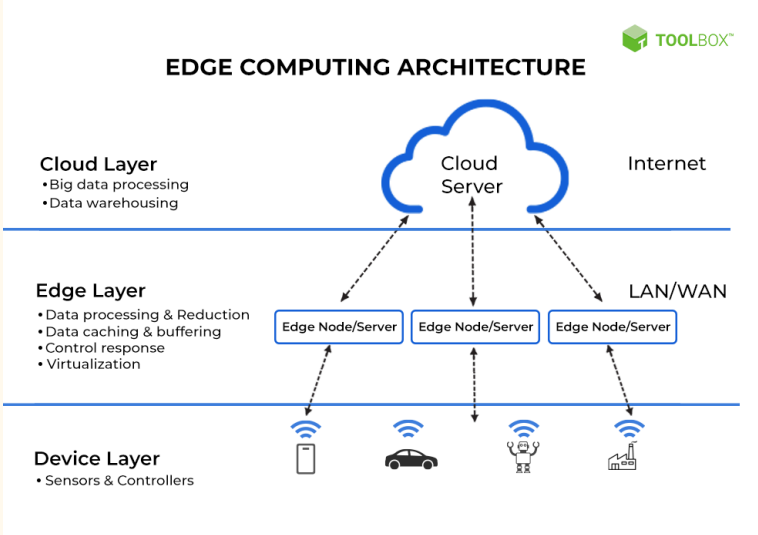


Figure 3: Edge Computing Architecture

The integration of IoT devices elaborates on the issues of data provenance and integrity. Without establishing a clear chain of custody for the evidence originating from devices across dispersed networks is challenging but crucial for the legal proceedings. The *Parliamentary Office of Science and Technology (2021)* highlights the significance of digital forensics within criminal investigations, highlighting the need for legal frameworks to work in tandem with technological advancements in order to address the challenges properly.

Legal and Regulatory Framework

The UK's legal and regulatory framework for edge computing is anchored by the Data Protection Act 2018 and GDPR, imposing rigorous standards on data privacy and security. Forensic practices within edge computing must navigate these regulations, ensuring the lawful processing and protection of personal data during investigations. The dynamic nature of edge computing, coupled with the UK's departure from the EU, introduces additional complexity, necessitating a reevaluation of cross-border data transfer mechanisms and international cooperation in digital forensics. As Al Mutawa et al. (2012) highlight, the legal challenges of multimedia data forensics in edge environments exemplify the broader issues faced by forensic investigators, calling for an intersection of legal acumen and technical expertise to uphold the principles of justice in the digital age.

Comparative Analysis

In Cloud computing, the forensic landscape is primarily governed by data jurisdiction and encryption standards as underscored by the Investigatory Powers Act 2016. This legislative piece, is demonstrative towards the UK’s actions on digital surveillance and data encapsulation, showcasing the complexity of the evidence gathering in the cloud, where data is able to traverse international boundaries. The multi-tenancy nature that comes with cloud computing settings, complicates the forensic process, due to the infrastructure sharing data between several devices. Because of this investigators have to be able to navigate a balance between accessing the sensitive data while keeping the privacy protections that are enshrined in the Data Protection Act 2018, and representing the GDPR principles.

Unlike Cloud Computing, the challenges that accompany Fog Computing are more granular. The short-lived nature of fog nodes[5] means that data is only able to exist momentarily, creating a need for immediate and precise forensic interventions. The judicial system within the UK, requires that digital evidence (which is now potentially dispersed across a number of intertwined nodes) to be collected and preserved with integrity. This system aligns with the discussion from *Casey (2011)*, regarding the need for a demonstrable chain of custody to be used.

Edge however, decentralises the data processing, which creates additional strains on the forensic investigations. Through the use and integration of IoT devices within edge computing helps magnify issues of data integrity, and the creation of a clear chain of custody, both being

pivotal during legal proceedings. The Parliamentary Office of Science and Technology (2021) highlights the significance of digital forensics during criminal investigations, proving the need for legal frameworks to evolve alongside the constant technological advancements of modern times. Comparatively, the framework Edge computing embodies is best shown by the same legal instruments that help guide both Cloud and Fog computing. However, the nature of Edge Computing, with its real-time processing and local storage, creates a more responsive forensic approach. This in turn reflects the issues that forensic investigators are facing, as further stated by Al Mutawa et al. (2012), who discusses the need for a fusion of both the legal and technical expertise.

Conclusion

The current adaptations of cloud, fog and edge computing has undeniably helped transform the digital landscape, allowing for unparalleled opportunities, innovation, and efficiency. These advancements, however, do come with challenges and frustrations, these are particularly seen within the realm of cyber-security and digital forensics. Throughout this essay I have explored each of the systems (cloud, fog, and edge) discussing each obstacle that investigators can encounter, from the difficulties of data jurisdiction and encryption in cloud computing, to the nature of data in fog nodes, and the decentralisation challenges that edge computing creates.

The difficulties when navigating through these environments highlight the need for robust forensic methodologies, legal frameworks, and technological solutions that can adapt to the constantly evolving digital world. The UKs current data protection laws and legal regulations such as the Investigatory Powers Act 2016 and the Data Protection Act 2018, stand at the forefront when addressing these challenges. However, the dynamic nature of cyber-crime, in tandem with the advancement of computing technologies, creates a need for a dialogue between these legal experts, technologists, and policy makers.

In conclusion, as the digital age continues to progress, the alignment of technological advancements with comprehensive legal frameworks is critical. Collaboration across sectors to allow for enhancement in forensic capabilities, while keeping privacy and data integrity, is necessary when maintaining the trust and security in the digital world. This essay has helped shed light on the complexities between technology and law in the cyber-crime atmosphere, highlighting the imperative for new solutions that can keep pace with the constant rapid improvements in cloud, fog and edge computing. As the digital world continues to develop, safeguarding digital integrity and a secure cyber environment will be the foundation in overcoming challenges posed by cyber-crime in these advanced computing systems.

Appendices

1. **Multi-tenancy** = *mode of operation of software where multiple independent instances of one or multiple applications operate in a shared environment.*

2. **Decentralising the data** = *By decentralising data, it improves speed and accessibility, so data is more discoverable.*

3. **Cross-border data flow** = *The movement or transfer of information between servers across country borders*

4. **Paradigm Shift** = *referring to a range of networks and devices at or near the user.*

5. **Nodes** = *the connection point among network devices such as routers, printers etc that can receive and send data from one point to another.*

References

- *Information Commissioner's Office, 2018. Data Protection Act 2018. [online] Available at: https://ico.org.uk [Accessed Date: 10th February 2024].*
- *Huntsman Security, 2022. Cyber crime and cloud computing: Security perspectives. [online] Available at: https://www.huntsmansecurity.com/blog/cyber-crime-and-cloud-computing-security-perspectives/ [Accessed Date: 10th February 2024].*
- *Zawoad, S., et al., 2017. Challenges of Network Forensic Investigation in Fog and Edge Computing. ResearchGate.*
- *Casey, E., 2011. Digital Evidence and Computer Crime. Academic Press.*
- *Peers, S., 2020. EU Law Analysis: The Future Relationship between the UK and the EU: The New UK-EU Trade, Cooperation and Fisheries Agreement.*
- *(No date) Definition of multitenancy - gartner information technology glossary. Available at: https://www.gartner.com/en/information-technology/glossary/multitenancy (Accessed: 10 February 2024).*
- *Decentralized Data: Definition, Data Products, Data Federation (2023) Starburst. Available at: https://www.starburst.io/learn/data-fundamentals/decentralized-data/#:~:text=Decentralized%20data%20architectures%20decouple%20the,the%20rest%20of%20the%20organization. (Accessed: 12 February 2024).*
- *(Accessed: 12 February 2024) Homepage | BSA | The Software Alliance. Available at: https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf (Accessed: 12 February 2024).*
- *Berry, T., 2010. Cloud computing: Forensic challenges for law enforcement. In Proceedings of the 2010 International Conference for Internet Technology and Secured Transactions, London, UK, 8-11 November 2010.*
- *Parliamentary Office of Science and Technology (POST), 2021. Digital Forensics and Crime. [online] Available at: https://post.parliament.uk/digital-forensics-and-crime/ [Accessed 10 October 2023].*
- *Al Mutawa, N., Bryce, J., Franqueira, V.N.L., Marrington, A., and Read, J.C., 2012. Forensics Investigations of Multimedia Data: A Review of the Challenges from a Legal Perspective. Journal of Digital Forensics, Security and Law, Vol. 7, No. 3.*
- *9, L.U.F. et al. (2022) What is cloud computing? definition, benefits, types, and Trends, Spiceworks. Available at:*

https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/ (Accessed: 12 February 2024).

- *Specialist, R.M.I. et al. (2022) What is fog computing? components, examples, and best practices, Spiceworks. Available at: https://www.spiceworks.com/tech/edge-computing/articles/what-is-fog-computing/ (Accessed: 12 February 2024).*
- *What is a network node? - it glossary (no date) SolarWinds. Available at: https://www.solarwinds.com/resources/it-glossary/network-node (Accessed: 15 February 2024).*
- *Specialist, Remya Mohanan IT et al. (2022) What is edge computing? components, examples, and best practices, Spiceworks. Available at: https://www.spiceworks.com/tech/edge-computing/articles/what-is-edge-computing/ (Accessed: 15 February 2024).*
- *Investigatory powers act 2016 (no date) Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (Accessed: 15 February 2024).*
- *Data protection act 2018 (no date) Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Accessed: 15 February 2024).*