A Critical Look at Distinguishing between the ‘cloud’, the ‘fog’ and ‘edge’ environments:

from the perspective of issues associated with obtaining and securing evidence in the investigation of cyber-crime.

Tags: cloud computing, fog computing, edge computing, forensic evidence, cybercrime.

Word Count: 2096 (excluding titles & references)

Contents

Figures & Tables

Introduction

When considering the collection of evidence in environments such as the cloud, fog and edge environments, the difficulties faced are glaringly obvious, the dynamic nature of these environments make it extremely difficult for the collection of evidence, impacted by encryption techniques and other security measures, as well as global laws, further complicating the process. (Damshenas et al., 2012a). There is a basic need with all law enforcement agencies to collect evidence when a crime is committed, this is essential activities for enablement of identifying crimes and their perpetrators, and additionally supporting civil matters, legislation and enforcement actions. With this paper we will explore the legal issues surrounding the gathering of evidence within these environments and look at the challenges faced by the forensic specialists in this setting. This will also look at setting out a brief explanation of each environment and take a look at the differences between them.

Defining The Cloud, The Edge, and The Fog

When looking at the differences between the cloud, fog, and edge computing, each have their own unique features to set them apart, and each have their own drawbacks when considering the collection of evidence. They offer a different architecture and provide resources for computer based environments. (Overby, n.d.), all with differing variations of services, uniquely named; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). (Birk, 2011.) When looking at cloud, fog and edge computing, there is two noteworthy differences, the proximity to users and to the source of the data each hold and/or require. Cloud computing is predominantly used for apps and data, that don't have the need for optimal latency, whereas fog and edge computing both need low latency and processing in real-time. The second set of differences are the devices, software and data they all service, Cloud is mainly for apps and data, fog is mainly used industrially and with IoT apps, and edge computing is mostly used for mobile and sensor apps. One thing that is prevalent in this research so far, cloud computing seems to offer the most security and control, which comes across as limited with fog and edge environments. ("Differences Between Cloud, Fog and Edge Computing," 2022)

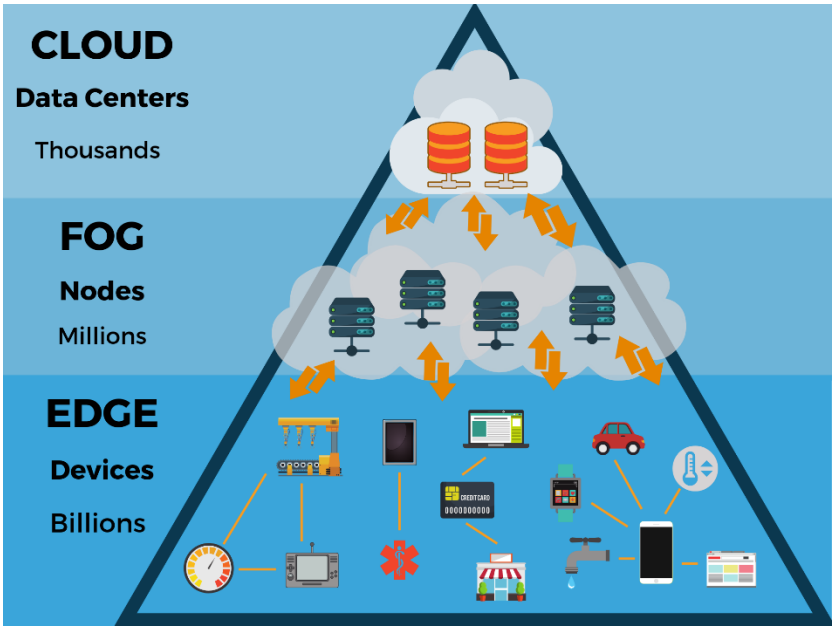

Figure 1. Depiction of the processes of Cloud, Fog, and Edge Computing, (http://www.thinkebiz.net and admin, 2019)

Cloud Computing

In simple terms, cloud computing offers computing services and resources without the need for costly infrastructure. That being said, companies that utilise cloud infrastructure are not always aware of what's behind this seemingly great technology, have they seen the premises, and have they considered the security, privacy and data implications of using this type of service. Another noteworthy point is to differentiate the two main

models, private and public cloud environments, with private being for one organisation, and public being for the many, additionally there are others including community cloud and hybrid cloud, but Birk points out that regardless of this, there will be limitations on how users control their own data. (Birk, 2011). According the Peter Mell and Tim Grance, authors of the definition of cloud computing at NIST, The definition of cloud computing 'is enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources' (Mell and Grance,(NIST) 2011).

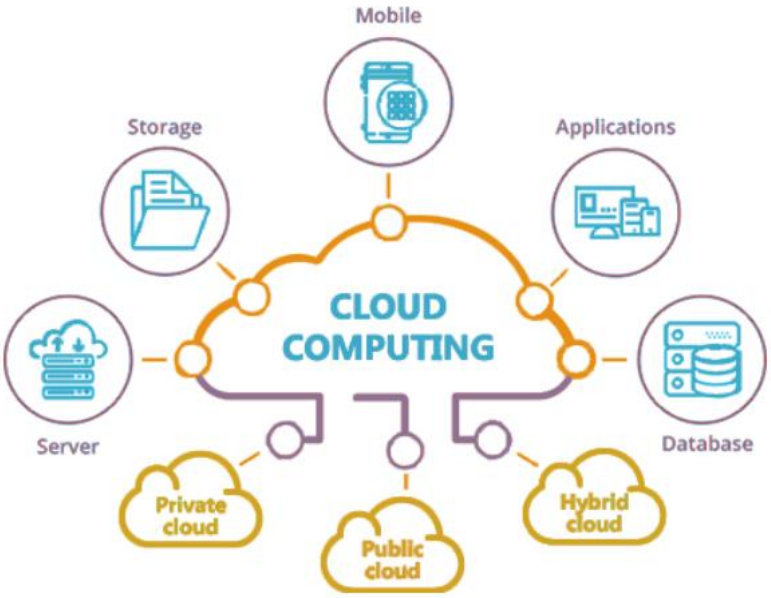

Figure 2. Depiction of Cloud Computing, (Baird, 2022).

Fog Computing

Fog computing is a distributed computing architecture that is designed to bring computing resources closer to the edge of the network, often in devices such as routers and switches. This allows for faster processing of data and applications, as well as reduced network congestion and latency. (Atlam et al., 2018). (Losavio, 2020) takes a look at how, Despite its benefits, Fog and Edge computing pose a very real and serious threat to the privacy of millions of people. Losavio pointedly remarks that generally with anything IOT (Internet Of Things) related, security becomes an afterthought with performance taking a front seat, this doesn't seem to be any different when it comes to cloud computing and directly impacts the ability to collect digital evidence. According to (Mukherjee et al., 2017), Cisco was the first company to try Fog Computing, and discusses in depth the challenges faced with privacy and security in fog computing; Cloud Computing offers its own challenges, and there has been time to deal with the vulnerabilities as best the world could. With these new proposals comes new risks and vulnerabilities.

(Hegarty and Taylor, 2021) takes a look at the digital complications that arise from utilising digital forensics in Fog Computing, such as, attempting to attain evidence relating to a single user almost impossible without also targeting other users data, this then brings about complications and is closely aligned with 'mass surveillance' and 'targeted law enforcement investigations'. In addition to this, fog computing will not save all of its data to ensure it keeps high performance and the desired speed.

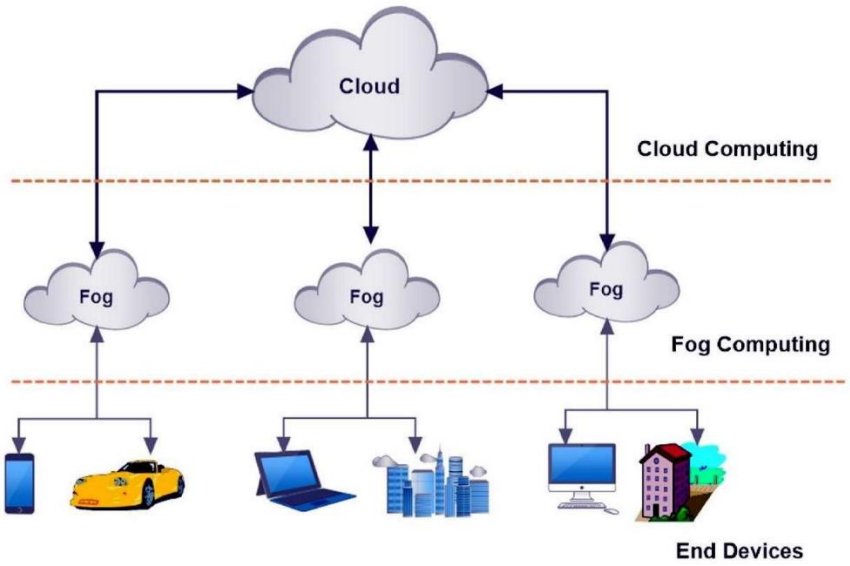

Figure 3. Depiction of Fog Computing, (Atlam, Walters and Wills, 2018).

Edge Computing

Edge computing involves the processing of data and applications close to its source, such as on a mobile device or in an IoT sensor. This allows for quicker and more responsive processing of data, this also reduces delay and can be useful in scenarios where network connectivity is limited or unreliable, meaning the closer the network is, the better the connection. (Soni et al., 2021). (Baird, 2022) Examples can be seen in the smart devices we all use, wear and love. Additionally Gartner posits that although as of now, only 10% of enterprise data is comprised at the edge, 'by 2025 that will grow to 75%'. ("What Edge Computing Means For Infrastructure And Operations Leaders," n.d.)

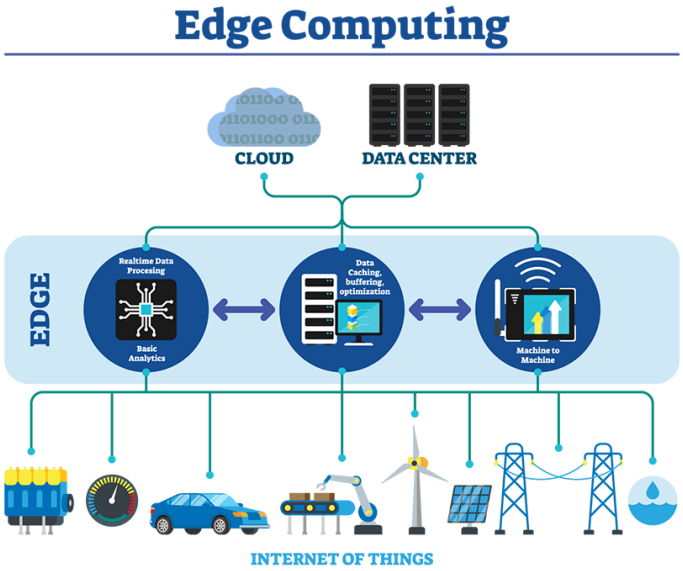

Figure 4. Depiction of Edge Computing, (Fong, 2019).

A Critical Look at the Relevant Laws Across the World

In cloud, fog, and edge computing, laws such as the General Data Protection Regulation ("General Data Protection Regulation (GDPR) – Official Legal Text," n.d.) and ("Guide to the UK General Data Protection Regulation (UK GDPR)," 2023) in the European Union and the("Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC," 2022) in the United States, set requirements for data protection, privacy, and security. Compliance with these laws is mandatory and failure to comply may result in legal and financial consequences for cloud service providers and their clients. It's important to consider worldwide laws when using any of these environments because there seems to be a large cross-over continents in business due to the decentralised nature of the cloud, fog and edge environments, for example, a business in the UK may be utilizing cloud infrastructure that have data centres in Europe or America, meaning for anything legal related, laws within each country must be followed.

Standards, such as the ISO/IEC 27000 and its family of guidelines can aid in protecting organisations and individuals, (ISO, 14:00-17:00, n.d.)and the ("Cybersecurity Framework," 2013). Both provide guidance on how to manage and secure cloud computing systems and services. These standards help ensure that cloud service providers implement appropriate security controls to protect their clients' and employees' data. In fog and edge computing, many of the same laws, standards, guidelines, procedures, and restrictions that apply to cloud computing also apply. However, there may be additional requirements for fog and edge computing systems due to their distributed and decentralised nature. For example, fog and edge computing systems may require additional security controls to protect data in transit and at the edge.

Data Protection Act 2018	This law governs the collection, use, and storage of personal data in the UK. It requires organisations to obtain informed consent from individuals before collecting their personal data and to implement appropriate security measures to protect that data.
Computer Misuse Act 1990	This law makes it a criminal offense to gain unauthorised access to a computer or network, or to cause damage to a computer or network without authorization.
Electronic Communications Act 2000	This law regulates the interception of electronic communications, including email and internet traffic.
GDPR	Although it is an EU regulation, the GDPR applies to UK businesses that process personal data of EU citizens. It sets out strict rules on how personal data should be processed, stored, and protected.
Investigatory Powers Act 2016	This law provides authorities with powers to monitor and intercept electronic communications in the interests of national security and the prevention of crime.
Copyright, Designs and Patents Act 1988	This law governs the protection of intellectual property, including software, music, and video.
Computer Programs and Data Copyrights Act 1988	This law provides legal protection for computer programs and databases in the UK. It makes it an offense to copy or distribute copyrighted material without permission. It also provides the framework for protecting software development and data ownership, including database rights. The Act applies to all computer programs, including those stored in the cloud, fog, and edge computing environments.
Human Rights Act 1998	This law incorporates the European Convention on Human Rights into UK law. It sets out fundamental human rights and freedoms that must be respected by public authorities, including law enforcement agencies. The Act protects individual privacy rights, which may be relevant in cases involving cloud, fog, and edge computing.
Freedom of Information Act 2000	This law provides public access to information held by public authorities. It allows individuals to request information from public authorities, including information stored in the cloud, fog, and edge computing environments. The Act requires public authorities to respond to requests for information within a set time frame and provides a framework for handling requests and appeals.
Consumer Rights Act 2015	This law governs consumer rights in relation to goods and services purchased online, including cloud computing services.
Network and Information Systems Regulations 2018	These regulations require organisations that provide essential services, such as energy, water, and transport, to take steps to improve the security of their network and information systems. The regulations apply to organisations that operate in the cloud, fog, and edge computing environments if they provide essential services. The regulations require organisations to assess and manage risks to the security of their network and information systems, and to report significant incidents to the relevant authorities.

Table.1. UK laws that are relevant to cloud, fog, and edge computing,("Legislation.gov.uk," n.d.).

Identifying Actions Contrary To Legal Requirements

This table highlights the many ways in which actions are identified contrary to legal requirements. There are many actions that may be contrary to legal requirements within the area of collecting sensitive information, such as evidence gathering. Organisations and individuals must ensure that they are complying with all relevant laws and regulations When dealing with cloud, fog, and edge environments, that also means making sure that they know which countries their provider operates in.

Collecting personal data without informed consent	Many data protection laws require organisations to obtain informed consent from individuals before collecting their personal data. Failing to obtain this consent can result in legal penalties.
Collecting sensitive personal data	Some types of personal data, such as health information, are considered "sensitive" and are subject to more stringent legal requirements. Collecting sensitive personal data without a legitimate reason or without proper safeguards can be a violation of data protection laws.
Sharing personal data without consent	In many cases, organisations are prohibited from sharing personal data with third parties without obtaining explicit consent from the individual. Sharing personal data without consent can be a violation of data protection laws.
Failing to properly secure personal data	Organisations have a legal obligation to protect personal data from unauthorised access or disclosure. Failing to implement appropriate security measures to protect personal data can be a violation of data protection laws.
Failing to properly dispose of personal data	Organisations must also take appropriate measures to dispose of personal data when it is no longer needed. Failing to do so can be a violation of data protection laws.
Failing to provide individuals with access to their personal data	Many data protection laws require organisations to provide individuals with access to their personal data upon request. Failing to provide this access can be a violation of data protection laws.
Discrimination based on personal data	Collecting and using personal data in a discriminatory manner, such as making decisions based on an individual's race or gender, can be a violation of antidiscrimination laws.

Table 2 – Identifying actions contrary to legal requirements

Existing Case Law

Here these cases highlight the legal and ethical challenges associated with cloud, fog, and edge computing. Organisations must be mindful of the potential risks and take steps to protect user privacy and comply with relevant laws and regulations. Additionally, the Microsoft v. United States and Schrems II cases highlight the challenges associated with cross-border data transfers outside of America. The Cloudflare v. Blackbird case demonstrates the potential impact of patent litigation on the cloud computing industry. The Microsoft vs United States case brought into the spotlight the difficulties faced in evidence collection in cross-border data access. The Cambridge Analytica Scandal, Google's Nightingale Project, Amazon's Facial Recognition Technology, and Apple's Siri Recordings, all used a cloud based service in their quest to harvest and analyse data.

Cambridge Analytica scandal	In 2018, it was revealed that the political consulting firm Cambridge Analytica had harvested the personal data of millions of Facebook users without their consent. This data was used to create targeted political ads during the 2016 US presidential election. The scandal raised questions about data privacy and the ethics of using personal data for political purposes. Wikipedia Contributors (2019a).
Google's Project Nightingale	In 2019, it was revealed that Google had partnered with the healthcare provider Ascension to collect and analyse the personal health data of millions of patients without their knowledge or consent. The project raised concerns about patient privacy and the potential misuse of personal health data. Schneble, Elger and Shaw (2020).
Amazon's facial recognition technology	Amazon has faced criticism for its facial recognition technology, which has been used by law enforcement agencies to identify individuals. Critics argue that the technology is biased against people of colour and violates civil liberties. Hao (2020).
Apple's Siri recordings	In 2019, it was revealed that Apple had been using contractors to listen to and transcribe recordings of Siri interactions. This raised concerns about user privacy and the ethics of using human contractors to analyse sensitive data. Su (2019).
Microsoft v. United States	In this case, Microsoft challenged a U.S. government warrant seeking access to customer data stored on servers located in Ireland. The case raised important questions about the jurisdiction of law enforcement agencies over data stored in the cloud and the privacy rights of individuals. Wikipedia Contributors (2019)
Schrems II	In this case, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield, a framework that allowed the transfer of personal data between the EU and the United States. The ruling had significant implications for cloud service providers, as it restricted the transfer of personal data to countries that do not provide adequate data protection. CJEU (2020).
Cloudflare v. Blackbird	In this case, Cloudflare sued Blackbird, alleging that Blackbird had engaged in a campaign of patent litigation against Cloudflare and other cloud service providers. The case raised important questions about the role of patent litigation in the cloud computing industry and the potential impact on innovation and competition. Goldberg (2017).

Table.3. Examples of Existing Case Law.(Damshenas et al., 2012b)

Real World Examples

These examples demonstrate that evidence gathering in the investigation of cybercrime within cloud, fog, and edge computing can be challenging but is possible with appropriate legal and technological expertise. In the Dropbox Hack, a cloud storage vulnerability led to this attack, but authorities managed to obtain a warrant for information which successfully led to a conviction. With the Mirai Botnet attack, IoT devices were compromised, investigators were able to track the perpetrators via analysis of the botnet network activities. The Capital One Data breach, who were using Amazon Web Services (AWS) cloud server to store data, were hacked by an ex-AWS engineer, Paige Thompson, who created a tool that scans data within the AWS architecture and used this data to hack the popular bank, evidence was collected from the server which led to a conviction.

The Dropbox Hack	In 2012, hackers gained access to Dropbox user accounts by exploiting a vulnerability in the company's cloud storage system. Law enforcement authorities investigated the hack and obtained a warrant to search the email account of one of the suspected hackers. The evidence collected from the email account helped to identify the individuals responsible for the attack. Gibbs (2017).
The Mirai Botnet Attack	In 2016, a massive botnet attack was launched against Dyn, a major provider of domain name system (DNS) services. The attack was conducted using the Mirai botnet, which was composed of compromised Internet of Things (IoT) devices. Law enforcement authorities investigated the attack and were able to track down the individuals responsible by analyzing the network traffic generated by the botnet. MalwareBytes (2016).
The Capital One Data Breach	In 2019, Capital One suffered a data breach that exposed the personal information of millions of customers. Law enforcement authorities investigated the breach and were able to track down the individual responsible by analyzing data stored on an Amazon Web Services (AWS) cloud server. The evidence collected from the cloud server helped to build a case against the suspect. Waldman (2022).

Table.4. Real-World Examples of Successful Evidence Gathering.

Technological Outcomes to Legal Requirements

Technological outcomes in cloud, fog, and edge computing can have important implications for legal requirements. Digital Forensic tools, Cloud Computing, Artificial Intelligence, Machine Learning, and Blockchain Technology all play a part in the potential technological outcomes for this technology.

When considering the collection of evidence in any cloud environment, the advancement of digital forensic tools can aid in ensuring a more streamlined and less complicated process for digital investigators. Cloud storage will develop further to allow for easy cross-border sharing and better cross-border relations in regard to legal cases that may cross paths of multiple countries. Incorporating Artificial Intelligence (AI) and Machine Learning (ML) can be utilised to gather large amounts of information in a particular data heavy criminal investigation and could help with identifying faces and objects in images and videos, and could possibly help to analyse financial data, and communications. Blockchain Technology can aid criminal investigations by supporting chain of custody with evidence collection, meaning it will be kept secure in a decentralised and distributed ledger, as well having a strong log of inputs, access, and alterations.

In essence, the technological advancements associated with cloud, fog, and edge computing have significant ramifications for legal obligations surrounding data protection, cross-border data transfers, intellectual property rights, and cybersecurity. Organisations can proactively address these issues by deploying appropriate technological measures that foster compliance with legal mandates. (Whalen, 2022).

Data protection and privacy	Cloud, fog, and edge computing technologies enable the storage and processing of substantial amounts of data, which can contain sensitive information. Legal requirements, such as the GDPR and CCPA, mandate that this data must be protected and processed in compliance with data protection and privacy laws. Technological outcomes, such as data encryption and access controls, can help to ensure compliance with these requirements.
Cross-border data transfers	Cloud, fog, and edge computing technologies can facilitate the transfer of data across borders, which can raise legal issues related to data protection and privacy. For example, the GDPR and Schrems II ruling require that personal data can only be transferred to countries that provide an adequate level of data protection. Technological outcomes, such as geo-fencing and data residency controls, can help organisations to comply with these requirements.
Intellectual property rights	Cloud, fog, and edge computing technologies enable the sharing and distribution of digital content, which can raise legal issues related to intellectual property rights. Technological outcomes, such as digital rights management and content fingerprinting, can help to protect the intellectual property rights of content owners.
Cybersecurity	Cloud, fog, and edge computing technologies can be vulnerable to cyber threats, which can compromise the confidentiality, integrity, and availability of data. Legal requirements, such as the HIPAA Security Rule and the EU Network and Information Systems Directive, mandate that organisations must implement appropriate cybersecurity measures to protect against these threats. Technological outcomes, such as network segmentation and intrusion detection systems, can help organisations to comply with these requirements.

Table.5. Technological Outcomes Considerations.

Issues Surrounding Evidence Gathering in the Investigation of Cyber-Crime

The impact of laws, standards, guidelines, procedures, and restrictions on the collection of forensic evidence in the UK, the USA, and Europe depends on the specific regulations in place in each jurisdiction. These regulations help ensure that forensic evidence is collected and analysed in a manner that is lawful, reliable, and admissible in court, that is not to say it isn't a difficult task and nor does it say that every country will like this collaboration, (Mowbray, 2009). (Damshenas et al., 2012) offers a solution to the difficulties faced in collecting forensic evidence, which could be stored on a myriad of different devices and locations, and with limited access to the physical devices to ensure evidence collected has integrity and thus giving admissibility in court, relating back to utilising blockchain technology could support this.

Data protection laws	Laws such as GDPR in the EU, the California Consumer Privacy Act (CCPA) in the USA, and the UK Data Protection Act (DPA) regulate the collection, processing, and storage of personal data. These laws may impact the collection of forensic evidence by requiring that personal data be collected and processed lawfully and fairly, and that appropriate security measures be in place to protect the data.
Privacy laws	In addition to data protection laws, there may be other privacy laws in place that impact the collection of forensic evidence. For example, in the USA, the Fourth Amendment of the Constitution protects individuals from unreasonable searches and seizures, which may impact the collection of forensic evidence by law enforcement.
Chain of custody procedures	To ensure that forensic evidence is admissible in court, chain of custody procedures must be followed. These procedures require that the evidence be properly documented and stored to maintain its integrity and reliability. Standards such as ISO/IEC 17025 provide guidelines for chain of custody procedures.
Digital forensic standards	Digital forensic standards such as the Digital Forensics Standard ISO/IEC 27037 provide guidance on the collection, examination, analysis, and reporting of digital evidence. These standards help ensure that forensic evidence is collected and analysed in a consistent and reliable manner.
Access to cloud data	In cloud computing environments, the collection of forensic evidence may be complicated by the fact that the data is stored remotely and may be subject to access control restrictions. Regulations such as GDPR and the DPA provide guidelines on how cloud service providers should handle requests for access to data.

Table.6. Collection of Evidence Impactions.

Critical Analysis & Conclusion

In this paper we have identified the differences between cloud, fog, and edge computing technology, we have discussed various legal issues related to cloud, fog, and edge computing, including data protection, privacy, and evidence gathering in cybercrime investigations. We also examined relevant legislation and case law at the national and international levels and the impact the said laws and investigations have on the collection of evidence and future investigations.

Noting that the distributed and dynamic nature of these systems can make it very difficult for forensic investigators to identify and preserve evidence in cloud environments, but with appropriate legal and technological expertise, investigators can successfully obtain the evidence necessary to build a case against cybercriminals. The legal issues related to the collection of evidence in cloud, fog, and edge computing are complex and multifaceted. That being said, there are technological advancements in the works whose purpose could make the lives of investigators much simpler.

The challenges faced everyday by investigators collecting evidence in this environment are many; from the complex legal barriers, and the multi-border regulations relating to privacy and data, all impacting the time it takes to gather evidence as well as jeopardising evidence integrity. The world of forensic investigations has a lot of potential for making these processes simpler and easier, with the technological advancements in general offering potential to build bridges cross-border lines and pose a significant increase in evidence integrity using blockchain technology.

References

Atlam, H., Walters, R. and Wills, G. (2018). Fog Computing and the Internet of Things: A Review. *Big Data and Cognitive Computing*, [online] 2(2), p.10. doi:https://doi.org/10.3390/bdcc2020010 Reference for image depiction of Fog Computing.

Baird, C. (2020). *A Primer on Cloud Computing*. [online] Medium. Available at: https://medium.com/@colinbaird_51123/a-primer-on-cloud-computing-9a34e90303c8 Source for Cloud Computing Depiction image.

Centers for Disease Control and Prevention (2022). *Health insurance portability and accountability act of 1996 (HIPAA)*. [online] Centers for Disease Control and Prevention. Available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

CJEU (2020). *AT A GLANCE*. [online] Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

CSA (2023). *Cloud Security Alliance*. [online] Cloud Security Alliance. Available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

Damshenas, M., Dehghantanha, A., Ahmed, R. and Shamsuddin, S. (2012). *Forensics Investigation Challenges in Cloud Computing environments.* [online] Available at: https://www.researchgate.net/publication/261160167_Forensics_investigation_challenges_in_cloud_computing_environments [Accessed 24 Feb. 2023]. Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012. 190-194. 10.1109/CyberSec.2012.6246092.

GDPR (2018). *General Data Protection Regulation (GDPR)*. [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

Gibbs, S. (2017). *Dropbox hack leads to leaking of 68m user passwords on the internet*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach.

Goldberg, J. (2017). *Blackbird Tech LLC v. Cloudflare, Inc., CIVIL ACTION NO. 17-283 | Casetext Search + Citator*. [online] casetext.com. Available at: https://casetext.com/case/blackbird-tech-llc-v-cloudflare-inc [Accessed 10 Apr. 2023].

GOV UK (2018). *Data Protection Act*. [online] Gov.uk. Available at: https://www.gov.uk/data-protection.

Hao, K. (2020). *The two-year fight to stop Amazon from selling face recognition to the police*. [online] MIT Technology Review. Available at: https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/.

Hegarty, R. and Taylor, M. (2021). Digital evidence in fog computing systems. *Computer Law & Security Review*, 41(41), p.105576. doi:https://doi.org/10.1016/j.clsr.2021.105576.

http ://www.thinkebiz.net, eBiz S. (2019). *What is Edge Computing? | Moving Intelligence to the Edge*. [online] eBiz Solutions, LLC. Available at: https://www.thinkebiz.net/what-edge-computing/ Reference for image depiction of cloud, fog and edge computing.

ICO (2022). *Guide to the General Data Protection Regulation (GDPR)*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

Innovation At Work (2019). *Real-Life Use Cases for Edge Computing*. [online] IEEE Innovation at Work. Available at: https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/ Reference for image Depiction of Edge Computing.

ISO (2013). *ISO/IEC 27001 Information security management*. [online] ISO. Available at: https://www.iso.org/isoiec-27001-information-security.html.

LexisNexis (2022). *Cloud computing—key legal issues | Legal Guidance | LexisNexis*. [online] www.lexisnexis.co.uk. Available at: https://www.lexisnexis.co.uk/legal/guidance/cloud-computing-key-legal-issues.

Losavio, M. (2020). Fog Computing, Edge Computing and a return to privacy and personal autonomy. *Procedia Computer Science*, 171, pp.1750–1759. doi:https://doi.org/10.1016/j.procs.2020.04.188.

MalwareBytes (2016). *What was the Mirai botnet*. [online] Malwarebytes. Available at: https://www.malwarebytes.com/what-was-the-mirai-botnet.

Mowbray, M. (2009). The Fog over the Grimpen Mire: Cloud Computing and the Law. *HP*, [online] 6(1). doi:https://doi.org/10.2966/scrip.x.x.

Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M.A., Choudhury, N. and Kumar, V. (2017). Security and Privacy in Fog Computing: Challenges. *IEEE Access*, 5(5), pp.19293–19304. doi:https://doi.org/10.1109/access.2017.2749422.

NIST (2019). *Cybersecurity Framework*. [online] NIST. Available at: https://www.nist.gov/cyberframework.

Overby, S. (2020). *How to explain edge computing in plain English*. [online] enterprisersproject.com. Available at: https://enterprisersproject.com/article/2019/7/edge-computing-explained-plain-english.

Schneble, C.O., Elger, B.S. and Shaw, D.M. (2020). Google's Project Nightingale highlights the necessity of data science ethics review. *EMBO Molecular Medicine*, 12(3). doi:https://doi.org/10.15252/emmm.202012053.

State of California Department of Justice (2023). *California Consumer Privacy Act (CCPA)*. [online] State of California - Department of Justice - Office of the Attorney General. Available at: https://oag.ca.gov/privacy/ccpa.

Su, J. (2019). *Confirmed: Apple Caught In Siri Privacy Scandal, Let Contractors Listen To Private Voice Recordings*. [online] Forbes. Available at: https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-apple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recordings/ [Accessed 10 Apr. 2023].

UK Legislation Database (2011). *Legislation.gov.uk*. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/search.

Waldman, A. (2022). *Paige Thompson found guilty in 2019 Capital One data breach*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/news/252521775/Paige-Thompson-found-guilty-in-2019-Capital-One-data-breach#:~:text=In%202019%2C%20Capital%20One%20confirmed.

Wikipedia Contributors (2019a). *Facebook–Cambridge Analytica data scandal*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

Wikipedia Contributors (2019b). *Microsoft Corp. v. United States*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States [Accessed 2 Aug. 2019].