Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 699 October 2024

Abstract | Transitioning to cloud-based infrastructure (CBI) for processing child sexual abuse material (CSAM) collected during police investigations could address resource challenges agencies currently face. While CBI provides quantifiable scalability and budgetary and inter-agency collaborative advantages, potential risks associated with data security, data sovereignty, and various legal and regulatory concerns may make agencies hesitant to make this transition. However, this paper demonstrates how a 'shared responsibility model' approach to cloud security can minimise risks, allowing investigators to take advantage of CBI benefits. In partnership with Oracle Corporation, we demonstrate how this could be implemented and continually monitored for new vulnerabilities within a CSAM context over time.

Benefits and risks of implementing cloud-based technology for child sexual abuse investigations in Australia

Bryce Westlake, Russell Brewer, Kellie Toole, Tom Daly, Thomas Swearingen, Scott Fletcher, Franco Ucci and Katie Logos

The volume of child sexual abuse material (CSAM)—including images, videos and audio recordings—being produced and disseminated by offenders represents a significant challenge for law enforcement investigations. This is because seizing, cataloguing, analysing and storing CSAM can be particularly laborious and traumatic (see Mitchell et al. 2022; Redmond et al. 2023; Strickland, Kloess & Larkin 2023). This has necessitated the development and uptake of myriad software services that can automate the processing of CSAM evidence at various points of the investigation—for example, breaking encryption of seized devices; identifying, extracting and matching intelligence (suspects' biometrics, locations, recording devices); and securely storing and retrieving CSAM. However, investigators have noted challenges associated with processing digital evidence quickly and at scale (Sanchez et al. 2019). In Australia this is exacerbated by a lack of hardware and other technological resources, such as data storage, along with the persistent challenges associated with sharing data across agencies

(Leclerc et al. 2022). These issues highlight the need for new methods that are scalable to the growing amount of CSAM evidence needing to be processed, and that also improve the capacity to share information across jurisdictions (Brown 2018). One such method is cloud computing, or cloud-based infrastructure (CBI).

CBI broadly encompasses a suite of interconnected technologies, including cloud-based hardware and software applications (for an overview, see Mell & Grance 2011). Despite CBI being viewed as both beneficial and viable for enhancing investigatory and analytical capabilities (Reilly, Wren & Berry 2011; Ridgeway 2018), the full potential of CBIs within CSAM contexts has not been realised. This is unsurprising, given the sensitive nature of CSAM evidence, coupled with potential security risks that may lead to trepidation by law enforcement agencies and non-government organisations processing CSAM. However, we argue that the benefits of cloud computing outweigh the associated risks, so long as appropriate and robust security strategies are designed, implemented and maintained.

Security within a CBI is accomplished through what is known as a shared responsibility model (SRM). Within this framework, responsibility for ensuring the security of the environment is shared between the cloud provider (eg Amazon Web Service, Azure, Oracle) and the customer (eg law enforcement agency). How an SRM is implemented can vary according to the cloud provider and the purpose of the CBI (see Lane, Shrestha & Ali 2017). However, traditionally, the cloud provider is responsible for the security *of* the cloud. This includes the host infrastructure (servers, storage space), network access control (policies and processes to protect against unauthorised access), and the physical data centre infrastructure (the building housing the host infrastructure). Conversely, the customer is responsible for the security *in* the cloud. This largely refers to data governance, including endpoint protection (security of the computers accessing the cloud) and user access management (controlling accounts on computers accessing the cloud). Depending on the service provided, the degree to which the customer and the cloud provider share responsibility for identity or access management (verification of users, access rights, issuing and denying of privileges) will differ.

In the current paper, we argue that CBIs can be a viable solution to technological resource challenges faced by agencies investigating CSAM. To support this argument, we begin by reviewing the discrete benefits of CBIs and assessing the perceived risks associated with their use. We then demonstrate how an SRM can work in practice by developing a secure cloud environment in partnership with one of the world's largest CBI providers, Oracle Corporation. Through this process, we illustrate how such an environment can be tailored to directly address the risks associated with CSAM, while simultaneously optimising the speed and cost associated with combating CSA. While the proposed secure cloud environment is intended to apply to various cloud-based implementations, we have framed our discussion around a cloud-based software application developed by the research team (see Westlake et al. 2022) to extract and match face and voice biometrics across CSAM files (Brewer et al. 2023). After providing an overview of the environment, we demonstrate its robustness through several security audits executed over a 45-day monitoring period. We conclude by offering insights into how CBIs can best be used and address some of the limitations associated with this approach.

Benefits of using CBI to combat child sexual abuse

A CBI can offer investigators a host of benefits that are not easily realised via alternative offline means. These benefits can be broadly classified into two types. The first relates to the elasticity of cloud computing, which includes potential cost reductions and increased speed, scalability and flexibility. The second relates to resource pooling and collaboration between users and agencies afforded by CBI. Each of these is elaborated upon in turn.

Elasticity: Improving scalability and performance while reducing costs

Substantive year-over-year increases in reported CSAM (National Center for Missing and Exploited Children 2022) necessitate continually increasing computer resources to analyse, evaluate and store CSAM evidence for future use (eg court cases). However, the costs associated with purchasing, operating and maintaining local hardware and software (including staffing costs) present significant budgetary challenges. These pressures can lead to reduced availability and reliability of potentially useful hardware and/or software resources, which can contribute to less efficient processing of evidence. Transitioning to CBI has the potential to reduce costs by moving the physical infrastructure required off-site, avoiding attendant maintenance and hardware failure responsibilities, while still allowing for effective scaling of capabilities as needed (Collins 2023). That is, resources such as processing power and storage capacity can be scaled up and down commensurate to needs, and can be adapted as circumstances change—for example, if additional processing power is required to rapidly process files from a large seizure. This could include ‘hard’ matching hash values to Interpol’s International Child Sexual Exploitation database or ‘perceptual’ hashing within Microsoft’s PhotoDNA; and identifying discrete objects through Griffeye Brain or the Australian Centre to Counter Child Exploitation’s ‘Trace an Object’ project. Enhancement of resource elasticity can lead to improved cost efficiency, access to tools otherwise inaccessible on local installations, and resource pooling between agencies to make investigations both faster and more comprehensive.

Resource pooling and collaboration

As the abuse of children and the materials produced and disseminated do not adhere to state, national or international borders, there is often a need to collaborate between agencies. Acknowledging this, law enforcement agencies around the globe have come together to adopt a coordinated approach to combatting child sexual abuse. In Australia, this has involved state and federal law enforcement agencies harmonising their efforts through Joint Anti-Child Exploitation Teams as well as the creation of the Australian Victim Identification Database. This coordinated approach has not only made it easier to share information among Australian agencies; it has also facilitated greater coordination of operations with international police forces and access to pertinent resources held by international agencies and non-government organisations (Australian Centre to Counter Child Exploitation 2019). Examples of the latter include Interpol’s International Child Sexual Exploitation database (Australian Federal Police 2022) and the Child Exploitation Tracking System (Homeland Security 2013), which integrates the Australian Victim Identification Database alongside other national databases to link criminal intelligence information together (CrimTrac 2010).

Complementing agencies' existing efforts, it is possible to augment the utility of these collaborative efforts via deeper integration of CBI services, which have the potential to increase the speed, reach and ease of sharing highly valuable information. This can best be accomplished using multi-tenancies, whereby a single application or database can be shared across multiple active users in real time. As such, each user or agency becomes a 'tenant' within the application or database and can directly (and instantaneously) leverage data provided by others (ie evidence from other cases or agencies), while also sharing their own, where appropriate. Adopting a holistic, real-time approach to investigations has distinct advantages over traditional interagency approaches, through an improved ability to draw new links between offenders, their associates and corresponding victims, which can improve investigatory outcomes, such as rescuing a child or arresting an offender more rapidly.

Risks associated with using CBI to combat child sexual abuse

While CBIs have distinct benefits, it is important to acknowledge that there are also potential security and legal risks. Given the sensitive and graphic nature of CSAM, it is essential for these risks to be fully considered and mitigated. Below we review the pressing risks associated with the use of CBIs in this context, including potential security vulnerabilities and challenges associated with navigating various legal frameworks.

Potential security risks

Extensive research conducted over the past decade has aimed to identify and mitigate cloud computing security risks. These have focused largely on privacy and confidentiality, access control, intrusion detection, securing virtual machines, encryption, and other potential vulnerabilities (for a full list, see Kumar & Goyal 2019). Nevertheless, review studies continue to identify numerous new or emerging security risks associated with cloud computing (eg Fatima & Ahmad 2019; George 2013; Morioka & Sharbaf 2016; Vistro et al. 2020). These risks are both general in nature (ie not unique to CBI, including misuse) and CBI-specific (ie a product of the CBI configuration). Maniah and colleagues (2019) have summarised these risks into four overarching categories:

- threats to applications, which include unauthorised access;
- threats to data, which include data breaches and data leakage;
- threats to cloud services, such as elevated privileges and misuse of cloud resources; and
- threats to infrastructure, which include insecure virtual machines and system or hardware failures.

We describe the first three, as they are most relevant to the adoption of CBIs for processing CSAM.

Threats to applications

One of the most significant threats to applications is account or service hijacking (ie unauthorised access), which can come from external or internal bad actors (Hashizume et al. 2013). For CSAM, this may be viewed as the greatest threat or hindrance in transitioning to CBI, as unauthorised access can introduce tangible legal risks for government and cloud providers (see *Potential legal risks*, below), while also contributing to further victimisation of abused children. When threats are external, they are most likely to occur because of social engineering tactics or weak credentials (eg passwords). However, they can also include cloud providers, their employees or other cloud users gaining unauthorised access. General internal threats may also come from rogue law enforcement investigators, who have legitimate access but are accessing restricted data outside of their required duties.

When examining CBI-specific threats, these can occur when external users obtain access through customer data manipulation, whereby attackers target web applications used to interact with the CBI, manipulating the data being sent (Ahmed et al. 2017). Threats to applications can be mitigated through CBI risk monitoring approaches such as appropriate user authentication procedures along with routine monitoring of privileges and access abnormalities, ensuring alerts are in place for when they occur and there exists a plan to quickly address them upon notification.

Threats to data

Most salient to threats to data are external breaches. These threats are considerable in a CSAM context, where a repository of potentially millions of videos and images could serve as an unintended 'honey pot' for those seeking to obtain a large amount of CSAM. Any such breach could cause significant harm, potentially resulting in server downtime, and consequences for the workforce (eg media scrutiny) as well as victims (eg revictimisation of children and additional dissemination). These threats can be classified as both general and CBI-specific risks, depending on the circumstances behind the breach—for example, did it occur because of social engineering?

While risk is ever-present, analysing more than 9,000 data breaches involving more than 12 billion records, Hammouchi and colleagues (2019) identified steps that can be undertaken to mitigate such threats. These include risk management approaches such as protecting against malware, ensuring access privileges are not disseminated through electronic means (eg email), preventing files from readily being downloadable, and monitoring and recording investigator actions. Beyond data breaches, one of the most common data security threats is 'leakage' (Choo 2010). This CBI-specific risk is where data are intercepted during the uploading, processing, storing and/or auditing stages. This is especially true when multiple tenants store data in the same database. To overcome this threat, data need to always be securely encrypted, with multi-factor authentication (MFA) protocols implemented, and procedures in place to rapidly identify and locate anomalies in data access.

Threats to cloud services

Threats to cloud services can arise from cloud providers having inadequate policies and procedures. Two common CBI-specific risks reported are elevated privileges and repudiation (Singh, Jeong & Park 2016). With elevated privileges, users have more access to CBI than necessary to complete their duties, while with repudiation there is a lack of controls to track and monitor user actions when using the CBI. Combined, these could impact the availability of services and misalign resources and responsibilities, leading to more access to a CSAM repository than is required or appropriate, without safeguards in place to monitor this access.

Related CBI-specific threats to cloud services are adverse events, such as incorrect installations or removal/failure of auditing and security alerts (Singh, Jeong & Park 2016), which can result from a weak service level agreement. The service level agreement serves as the foundation for expectations between the user (eg the law enforcement agency) and the cloud provider (eg Oracle) pertaining to cloud availability (eg 'up-time'), data ownership, backups and user responsibilities (Chang, Kuo & Ramachandran 2016). To overcome these CBI-specific threats to cloud services, it is imperative that an effective service level agreement is implemented that operates with a separation of duties and principles of non-repudiation and least privilege.

Potential legal risks

In addition to the risks associated with security, investigators or agencies need to be aware of, and compliant with, federal and state-based legal frameworks. These legal frameworks cover multiple areas pertaining to criminal law, the handling of evidence and data sovereignty.

In Australia, both federal and state law uniformly prohibit child sexual abuse, as well as accessing, possessing or transmitting any materials depicting any such abuse (eg images and videos, whether streamed or saved, as well as text; see *Appendix* for a list of relevant legal frameworks). Moreover, South Australia (s 63AB), Queensland (s 228DA), Victoria (s 51E), New South Wales (s 91HAA) and the Commonwealth (s 474.23) expressly prohibit 'administering' or 'hosting' websites or other digital platforms that are used to disseminate CSAM. Heavy penalties are prescribed in all jurisdictions (including lengthy custodial sentences) and this must be taken seriously when considering the implementation of a CBI. That is, using CBIs means using off-site computational resources maintained by a third-party cloud provider and this will invariably involve the storage of CSAM and transmission of CSAM between law enforcement and the cloud provider.

This is not to say that such arrangements are prohibited under Australian law. Rather, most jurisdictions stipulate circumstances under which an offence is *not* committed, and where such actions are justifiable and defensible, including where authorised police officers are acting in good faith and in the performance of their duties, and where a person is acting in good faith and for public benefit, including in assisting the administration of the criminal justice system or for a genuine child protection function (see *Appendix* for exemptions/defences). Accordingly, the use of CBIs for law enforcement purposes is permissible under Australian law and can indemnify cloud providers and law enforcement officers using CBIs from prosecution in most Australian jurisdictions. Only the Australian Capital Territory has no such exemption or defence.

Beyond criminal law, it is essential to consider other standards and frameworks governing police handling of digital evidence. This is particularly relevant given the volatile nature of electronic evidence (files can be easily or automatically altered/corrupted/deleted), and the potential for hardware failure. As such, any CBI implemented should be compliant with national standards (ie *Guidelines for the management of IT evidence*; Standards Australia 2003), and prescribed requirements outlined under applicable laws and regulations pertaining to the management of evidence. The requirements outlined in these frameworks vary considerably across jurisdictions, with some being more explicit than others about the management of digital evidence (as opposed to physical evidence). For example, the *Australian Federal Police Act 1979* (Cth) directs the *AFP National Guideline on Property and Exhibits*, which provides clear guidance with respect to the implementation of robust file-handling protocols for processing, copying and archiving digital evidence, to minimise the potential for damage, alteration or data loss (paragraph 14.2), as well as managing sexually explicit material, such as CSAM (paragraph 15). In contrast, a 2018 audit of Victoria Police processes indicated a lack of clear guidelines for evidence handling and highlighted the complexity of constructing such guidelines based on the need to synthesise at least 19 different pieces of relevant legislation (Victorian Auditor-General's Office 2018).

Considering the sensitivities associated with CSAM, there also may be legal implications with respect to the physical location of CBI data centres. In fact, the Department of Home Affairs (2018) recommends that government entities carefully consider matters of data sovereignty (ie data centre ownership, operation and control) when contracting third-party cloud providers and assess the need for the localisation of data centres where appropriate. Moreover, when assessing cloud providers, agencies should also review compliance with relevant certification frameworks, such as the federal Hosting Certification Framework (Digital Transformation Agency 2020), or state-based measures where appropriate (eg in NSW, procuring agencies must be compliant with the NSW Cyber Security Policy; Mitchell & Samlidis 2022).

Such precautions are for good reason: Australian criminal laws pertaining to CSAM (see *Appendix*) apply to offences committed within Australia. The 'extraterritorial' application of Australian criminal laws to crimes committed in another country presents challenges under constitutional and international law. The external affairs power in s 51(xxix) of the Australian Constitution does empower the Australian Parliament to legislate extraterritorially, and the *Criminal Code Act 1995* (Cth) includes child sexual offences committed outside of Australia. However, the current provisions require some connection with Australia, such as the citizenship or residency of the suspected offender (s 272.6), although there is some authority that similar laws do not require any connection to Australia (*XYZ v Commonwealth* (2006) 227 CLR 532, 547–8). Furthermore, the states and territories are not empowered to legislate extraterritorially, and extradition proceedings would be required to prosecute CSAM offenders from outside Australia under their laws. Data stored extraterritorially will also be subject to foreign legal frameworks, which may introduce additional privacy-related considerations and may not provide the same protections against prosecution when dealing with sensitive and potentially harmful personal data, such as CSAM (Mitchell & Samlidis 2022).

Where data are shared both across Australian jurisdictions and with international partners, it is important that practitioners adhere to the appropriate criminal intelligence sharing legislation. However, these laws and policies involve various complexities. For example, across all states and territories, there is an absence of clear legal definitions for what constitutes 'criminal intelligence' (Brown 2018). More specifically, it is not defined in the *Data Availability and Transparency Act 2022* (Cth) or the *Australian Crime Commission Act 2002* (Cth). However, section 36A of the *Australian Crime Commission Act 2002* (Cth) defines 'criminal intelligence assessment' as assessing whether a person '(a) may commit a serious and organised crime; or (b) may assist another person to commit a serious and organised crime'. Additionally, there are inconsistent information-sharing policies across jurisdictions (with a different legal framework governing each state and territory), and there is the application of agency-specific rules or specific terminology within such rules that is difficult to generalise and apply cross-jurisdictionally (Chan, Logan & Bennett Moses 2022).

Developing a secure environment to mitigate risks

The potential security and legal risks described above necessitate the development of a tailored security environment for processing and storing CSAM within an Australian setting. This environment must satisfy three objectives:

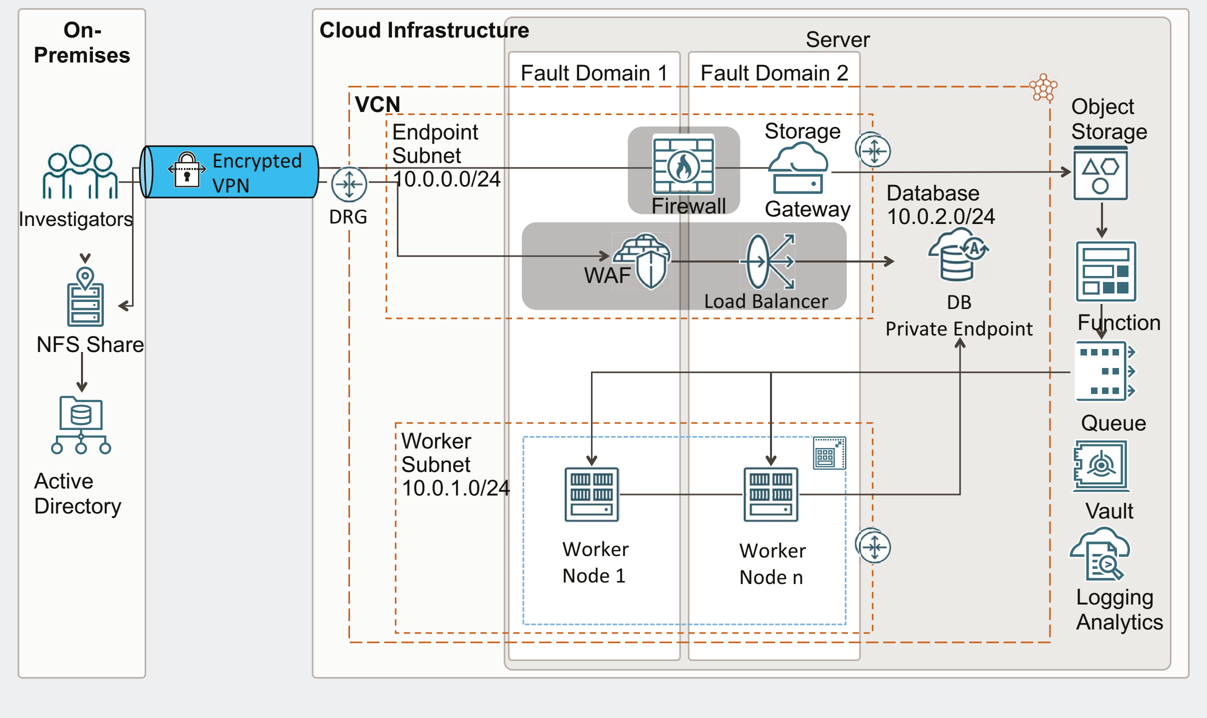
- objective 1—the CBI must meet or exceed operational and data security standards and effectively handle security threats and incidents;
- objective 2—the CBI must ensure that data reside within an appropriate jurisdiction and are only shared with approved users (ie specific agencies); and
- objective 3—the CBI must be protected from unauthorised access by third parties, internal bad actors (eg rogue law enforcement officers) and cloud provider employees, without impeding or slowing down investigatory workflows.

Considering the three objectives, we developed an example secure environment in collaboration with Oracle Corporation, framed around a highly scalable exemplar Python application created by the research team (Westlake et al. 2022). This application extracts and matches face and voice biometrics across child sexual abuse media files, and stores results in a database for subsequent review by investigators. Within the example environment implemented for this study, responsibility was shared. That is, Oracle assumed responsibility for ensuring that the environment exceeded industry and Australian standards for operational and data security (objective 1); that the data remained encrypted during access and storage, while monitoring and maintaining logs of access (objective 2); and that the network was secure, ensuring only the necessary ports were open and accessible (objective 3). Meanwhile, the customer (ie the research team) took responsibility for addressing security threats and incidents when flagged by Oracle (objective 1); issuing and revoking user access, implementing MFA, and forcing users to updated passwords regularly (objective 2); and maintaining security of the computers used to access the cloud environment at the agency, along with reviewing access logs and addressing anomalies identified (objective 3). Given that the security of the environment was being tested, no CSAM was housed within the environment.

Securing the environment (objective 1)

Figure 1 provides a high-level overview of the security environment developed. This environment adheres to international compliance certifications and assessment standards, including those of the International Organization for Standardization (ISO 27001), System and Organization Controls (SOC 1, 2 and 3), the Information Security Management System, and Infosec Registered Assessors Program requirements. Specific to Australia, the environment also complies with the Digital Transformation Agency's (2023) Hosting Certification Framework, which provides the latest certification framework for cloud providers of Australian Government data-hosting services. This environment involves a suite of tightly connected technologies (hardware and software), permitting the investigator to securely process and access their data using CBI. The interaction between these technologies is complex and is elaborated upon below.

Figure 1: Proposed cloud architecture for processing CSAM



Processing data (objective 2)

Investigators begin by placing the media files they wish to process in an NFS share (a network accessible file system with an active directory) located at law enforcement offices. A secure private connection (with no access to or from the internet and using 256-bit encryption) is then made between the NFS share and CBI and facilitated through a dynamic routing gateway, which directs traffic to resources within the CBI (see Oracle 2023a). The dynamic routing gateway routes traffic into a customisable virtual cloud network (which provides a secure and isolated environment for running cloud resources) and then into a dedicated endpoint subnet (see Oracle 2023b), which exists entirely within a secure data centre (in this case, in Sydney, NSW). Once routed through the endpoint subnet, data are processed through a firewall and storage gateway (a bridge between the on-premises storage and the cloud storage), before being entered into a data storage architecture known as Object Storage, which is optimised for use in cloud environments (see Oracle 2023c). In our implementation, the Object Storage upload permissions are set as write-only, thus permitting data to be uploaded for processing but preventing subsequent data retrieval. That is, data cannot be downloaded from Object Storage by anyone, including internal bad actors. A function (a code that performs a specific task) then enters the uploaded data into an encrypted processing queue. Data are then directed into a dedicated (private) worker subnet, containing several managed kubernetes cluster worker nodes (see Oracle 2023d). Here, the biometric features are extracted from the uploaded media files by the Python programs running in the worker nodes and subjects (victims/offenders) are identified and matched (Brewer et al. 2023). Match results are then sent to the database and can be later queried by investigators from designated locations via the above mentioned private encrypted network connections.

Accessing data (objective 3)

To access the processed data for analytical purposes, investigators will use a graphical user interface that directly accesses the CBI via an encrypted connection and queries the database to return results. This is accomplished via the dynamic routing gateway directing traffic through a web application firewall, which protects against malicious and unwanted internet traffic, and then through a load balancer, to distribute load to and from the interface and the database (containing match data).

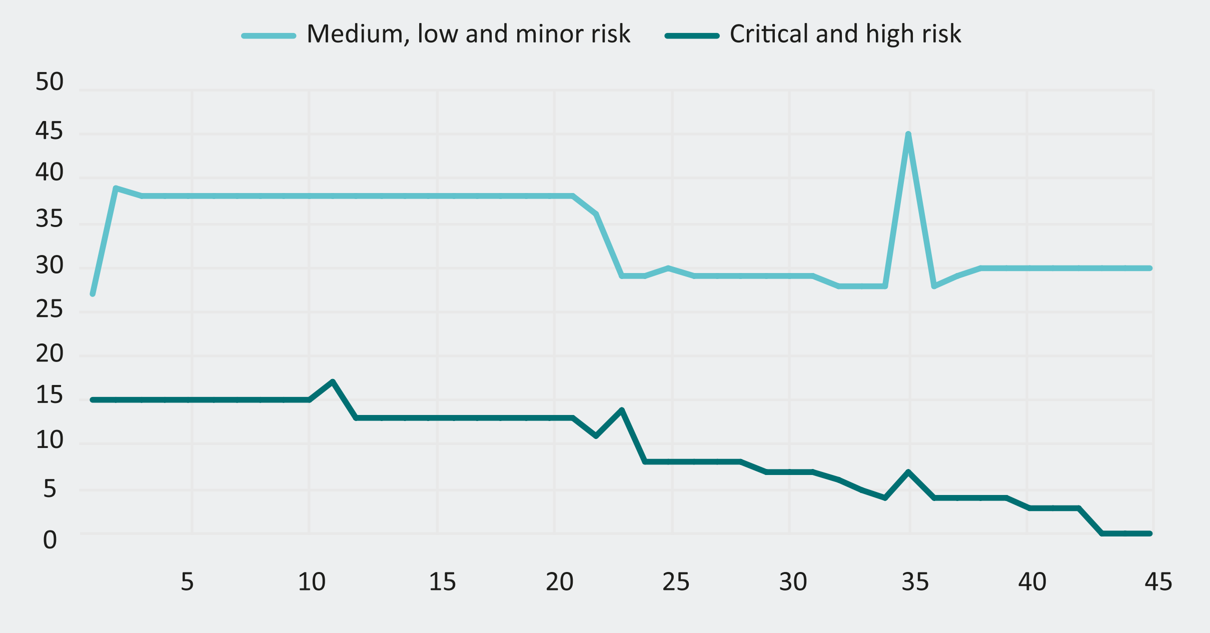
Underpinning this environment—whether for processing or accessing—are numerous other security, reliability and scalability features that have been implemented with an SRM in mind:

- multiple authentication and identification factors—stringently enforced access credentialing such as location verification (eg authentication with on-premises active directory to upload files), and enforced strong password policies, via robust identity and access management domains, with adaptive security (ie based on user behaviour, such as their previous login patterns, access device history etc);
- adoption of a least privilege framework—user/service access permissions are carefully constructed and set to 'deny' by default, with management groups (users, security administrators, developers) only having access to appropriate components, which remain independent of one another;
- multiple fault domains—separate processing instances are never operating on the same physical hardware at a given time. This ensures that maintenance activities or hardware failures (on the provider side) do not affect the entire environment and restrict law enforcement access or disrupt processing;
- logging analytics—security incident and event management monitoring is implemented across the full environment. All activities within the Cloud Infrastructure (see Figure 1) are logged, including any time the database is accessed. Anomalies and unusual activities in database access are flagged and reported to appropriate parties (on the provider and user side);
- user-managed encryption—user data are always encrypted using user-managed keys. It is critical that the cloud provider does *not* have access to these keys. This also renders data irretrievable should a key be intentionally deleted by law enforcement. Keys and other user credentials are stored in a cryptographically secure vault that meets international validation standards and benchmarks (ie FIPS 140-2). Plaintext (ie unencrypted communication on the network) is disabled by default.
- break-glass fail-safe—the environment contains a 'break-glass' account that can be given to a senior supervisor. This serves as a fail-safe measure that allows for immediate deletion of the database and any other data should it be needed.

Monitoring and maintaining robust operational security

Monitoring and assessing the security of a CBI implementation is not, and cannot be, a static process. Rather, it is an ongoing operational process that must be conducted by the customer in collaboration with the cloud provider. To demonstrate the robustness of the secure environment, the research team undertook a series of audits. An initial independent audit was conducted by Orca Security (https://www.orca.security), which identified zero critical/high risks. While it did identify 42 medium risks, these would be addressed by implementing an MFA procedure for all users, removing public accessibility to the database (ie via the internet), and updating passwords for accounts that were not intended to be a part of the operational environment. Within an SRM, 'flagging' these issues would be the responsibility of the cloud provider while addressing them would be the responsibility of the customer. Over 45 days (27 June to 10 August 2023) an ongoing audit was conducted every four hours by Oracle's built-in Cloud Guard (Oracle 2023e) and the outstanding risks are plotted in Figure 2.

Figure 2: Outstanding vulnerabilities over a 45-day period, by risk rating (according to Cloud Guard)



Cloud Guard identified 42 vulnerabilities on Day 1 of the observation period, with some (eg MFA) overlapping with Orca Security's report and others being unique (eg greater than needed user privileges). Of these, 15 were deemed critical/high risk with the remaining 27 medium/low/minor. Throughout the next 44 days, 40 additional vulnerabilities arose, with nine classified as critical/high risk and 31 as medium/low/minor. Throughout the observation period, the research team reviewed identified vulnerabilities, assessed whether action was needed and took appropriate steps to address the vulnerabilities. This process, along with the emergence of 'new' security vulnerabilities, is visible in the various spikes and drops in both the medium/low/minor and critical/high risk lines in Figure 2. This evolution reinforces that cloud security needs to be an ongoing process. At the conclusion of the 45-day observation period, all 24 critical/high risks and 28 of the 58 medium/low/minor risks (eg users having excessive privileges, old API keys) had been addressed. In an operational setting, the remaining 30 medium/low/minor risks would be addressed; however, within the current study, these were left as the research team needed public access, test accounts, generic passwords, and accounts without MFA for evaluation.

A second Orca Security audit was conducted at the conclusion of the observation period, which confirmed the finding of the Cloud Guard audit that there were zero critical/high vulnerabilities. While it reported 72 medium risks, 54 related to public accessibility and 17 to disabled MFA, which were required for testing purposes but would have been resolved were this an actual operational setting.

Discussion and conclusion

The abundance of intelligence information gathered in CSAM investigations necessitates new methods to effectively process and analyse evidence. The uptake of these methods has significant implications for the availability of adequate computing resources and can lead to cascading costs for law enforcement agencies. Moreover, the human costs are significant, both in terms of the adverse impact on investigators and inevitable delays in rescuing children being victimised. Due to these issues, we argue that wider adoption of CBIs in CSAM investigatory contexts has the potential to improve the speed of investigations and reduce the short- and long-term cost of computing infrastructure and maintenance, while facilitating mutually beneficial inter-agency collaboration. Within an SRM, ongoing vulnerability auditing capabilities allow customers to constantly monitor their environment in real time and collaborate with the cloud provider to adequately assess and address new vulnerabilities. This is an important advantage over traditional in-house security practices in law enforcement agencies, where missing MFA, outdated passwords and user accounts, excessive user privileges, suspicious activity and other vulnerabilities may go undetected and therefore unaddressed.

We acknowledge that the risks associated with CBIs can never be completely eliminated and that such concerns may lead law enforcement agencies to approach CBI with trepidation. The increasing uptake of CBI in high-volume computing contexts means that they will remain a target of bad actors. However, the centrality of CBI in modern computing also means that research on how to best identify and then mitigate new threats as they appear will remain a priority for cloud providers (Tabrizchi & Rafsanjani 2020). The external security audit conducted during the current research demonstrates the continued effort to quickly identify threats and highlights how they can be addressed. Each of the remaining risks, and new vulnerabilities that emerge, can be effectively managed through customers (eg law enforcement) and cloud providers assuming shared responsibility for planning, maintaining and monitoring the security environment. However, for this model to be effective, trust between the customer and the cloud provider is paramount. Central to this is ensuring that the customer is aware of the security practices they are responsible for, and which are the responsibility of the cloud provider. Therefore, it is imperative that any agreement or contract between the two organisations is clearly defined. Otherwise, one of the biggest pitfalls of this model is that responsibility could lie with no one. Providing such trust can be established, a CBI operated via an SRM has the potential allow investigators to harness the distinct benefits of the cloud to combat child sexual abuse, while continually monitoring and mitigating any downside risks.

Even if a CBI framework is adopted for CSAM investigations, we note that work is needed to ensure that the full potential of the technology is realised. For example, we acknowledge that one of the distinct benefits of CBI—the adoption of *real-time* information-sharing practices—may represent a break from traditional inter-agency procedures and frameworks. We argue, however, that this is a much needed step, agreeing with Brown (2018) that adopting more robust intelligence-sharing practices has the potential to reduce 'linkage blindness' (ie circumstances where one jurisdiction may either guard data or fail to share data), and thus improve investigator decision-making processes. Such adoption must take care not to replicate historical (but still common) intelligence-sharing mistakes, which often involve taking a measured approach, sharing only low-value intelligence (Coyne, Shoebridge & Zhang 2020). We stress that the only way to realise the full resource-pooling benefits of CBI will be the widespread (national and international) and uniform sharing of high-value intelligence from the outset. Falling short will result in a missed opportunity for law enforcement agencies to greatly enhance their investigative workflows and practices, while reducing financial costs.

We also acknowledge that this study has several limitations that should be addressed in future research. First, while the approach taken demonstrates that transitioning to CBI has merit in child sexual abuse contexts, we stress that the environment introduced in this paper may not be suitable for all CBI implementations or applications. We recognise that, given the sensitive and international nature of this problem, unique measures and requirements relating to software sharing, data storage and retention, and jurisdictional access may need to be considered. Any such planning should again be undertaken in consultation between the law enforcement agency and cloud provider and enshrined in formal agreements. Future research should seek to develop and audit alternative implementations.

Finally, while the security audits undertaken here effectively identified known vulnerabilities in line with international standards for best practice, additional testing of the environment prior to implementation would provide an additional layer of assurance for both law enforcement agencies and cloud providers. For example, third-party penetration tests (ie ethical hacking) simulate real-world attacks in a controlled environment and can be used to identify weaknesses that could be exploited by attackers. Future implementations of this environment should therefore endeavour to undertake such proactive testing in line with accepted methods and procedures (see Shah & Mehtre 2015 for an overview of methods). Engaging in these risk identification techniques can improve the reliability of the CBI, reducing system failures (Tian, Tian & Li 2020) and misconfiguration of users, database exposure and audit logging (Torkura et al. 2021).

References

URLs correct as at June 2024

Ahmed HAS, Ali MH, Kadhum LM, Zolkipli MF & Alsariera YA 2017. A review of challenges and security risks of cloud computing. *Journal of Telecommunication, Electronic and Computer Engineering* 9(1–2): 87–91. https://jtec.utem.edu.my/jtec/article/view/1662

Australian Centre to Counter Child Exploitation (ACCCE) 2019. Blueprint 2019–2021. Australian Centre to Counter Child Exploitation. https://www.accce.gov.au/what-we-do/about-us#Blueprint

Australian Federal Police 2022. Major upgrade to database a 'game changer' in tracking down online predators. https://www.afp.gov.au/news-centre/media-release/major-upgrade-database-game-changer-tracking-down-online-predators

Brewer R, Westlake B, Swearingen T, Patterson S, Bright D, Ross A, Logos K & Michalski D 2023. Advancing child sexual abuse investigations using biometrics and social network analysis. *Trends & issues in crime and criminal justice* no. 668. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78948

Brown R 2018. Understanding law enforcement information sharing for criminal intelligence purposes. *Trends & issues in crime and criminal justice* no. 566. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti101440

Chan J, Logan S & Bennett Moses L 2022. Rules in information sharing for security. *Criminology & Criminal Justice* 22(2): 304–322. https://doi.org/10.1177/1748895820960199

Chang V, Kuo YH & Ramachandran M 2016. Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems* 57: 24–41. https://doi.org/10.1016/j.future.2015.09.031

Choo KKR 2010. Cloud computing: Challenges and future directions. *Trends & issues in crime and criminal justice* no. 400. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti281703

Collins CE 2023. *Cloud storage and digital forensic evidence: Understanding misconceptions and providing answers.* Lake Jackson Police Department

Coyne J, Shoebridge M & Zhang A 2020. National security agencies and the cloud: An urgent capability issue for Australia. *Australian Strategic Policy Institute*. https://www.aspi.org.au/report/national-security-agencies-and-cloud-urgent-capability-issue-australia

CrimTrac 2010. *CrimTrac submission to the Legal and Constitutional Affairs Committee inquiry into the Crimes Legislation Amendment (Sexual Offences Against Children) Bill 2010*. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Completed_inquiries/2008-10/crimessexualoffences/submissions

Department of Home Affairs 2018. Protective Security Policy Framework. https://www.protectivesecurity.gov.au/

Digital Transformation Agency 2023. Hosting Certification Framework. https://www.dta.gov.au/our-projects/hosting-strategy/hosting-certification-framework

Fatima S & Ahmad S 2019. An exhaustive review on security issues in cloud computing. *KSII Transactions on Internet & Information Systems* 13(6): 3219–3237. http://doi.org/10.3837/tiis.2019.06.025

George B 2013. Security issues in cloud computing. *International Journal of Advanced Research in Electrical, Electronic and Instrumentation Engineering* 2(S1): 631–635. https://www.ijareeie.com/special-issue-december-13

Hammouchi H, Cherqi O, Mezzour G, Ghogho M & El Koutbi M 2019. Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science* 151: 1004–1009. https://doi.org/10.1016/j.procs.2019.04.141

Hashizume K, Rosado DG, Fernández-Medina E & Fernandez EB 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications* 4(5). https://doi.org/10.1186/1869-0238-4-5

Homeland Security 2013. Immigration and Customs Enforcement: Child Exploitation Tracking System. https://www.dhs.gov/publication/dhsicepia-017a-immigration-and-customs-enforcement-child-exploitation-tracking-system

Kumar R & Goyal R 2019. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review* 33: 1–48. https://doi.org/10.1016/j.cosrev.2019.05.002

Lane M, Shrestha A & Ali O 2017. Managing the risks of data security and privacy in the cloud: A shared responsibility between the cloud service provider and the client organisation. *The Bright Internet Global Summit*, Seoul

Leclerc B, Cale J, Holt T & Drew J 2022. Child sexual abuse material online: The perspective of online investigators on training and support. *Policing: A Journal of Policy and Practice* 16(1): 762–776. https://doi.org/10.1093/police/paac017

Maniah, Abdurachman E, Gaol FL, Soewito B 2019. Survey on threats and risks in the cloud computing environment. *Procedia Computer Science* 161: 1325–1332. https://doi.org/10.1016/j.procs.2019.11.248

Mell P & Grance T 2011. *The NIST definition of cloud computing.* Report no. SP 800-145. National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/145/final

Mitchell AD & Samlidis T 2022. Cloud services and government digital sovereignty in Australia and beyond. *International Journal of Law and Information Technology* 29(4): 364–394. https://doi.org/10.1093/ijlit/eaac003

Mitchell KJ, Gewirtz-Meydan A, O’Brien J & Finkelhor D 2022. Practices and policies around wellness: Insights from the Internet Crimes Against Children Task Force Network. *Frontiers in Psychiatry* 13. https://doi.org/10.3389/fpsyt.2022.931268

Morioka E & Sharbaf MS 2016. Digital forensics research on cloud computing: An investigation of cloud forensics solutions. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)*. Waltham, MA: 1–6. https://doi.org/10.1109/THS.2016.7568909

National Center for Missing and Exploited Children 2022. *2021 annual report*. https://www.missingkids.org/footer/about/annual-report

Oracle 2023a. Dynamic routing gateways. https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingDRGs.htm

Oracle 2023b. Virtual cloud network. https://www.oracle.com/cloud/networking/virtual-cloud-network/

Oracle 2023c. Overview of Object Storage. https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm

Oracle 2023d. Container engine for kubernetes. https://www.oracle.com/cloud/cloud-native/container-engine-kubernetes/

Oracle 2023e. Cloud Guard. https://www.oracle.com/security/cloud-security/cloud-guard/

Redmond T, Conway P, Bailey S, Lee P & Lundrigan S 2023. How we can protect the protectors: Learning from police officers and staff involved in child sexual abuse and exploitation investigations. *Frontiers in Psychology* 14. https://doi.org/10.3389/fpsyg.2023.1152446

Reilly D, Wren C & Berry T 2011. Cloud computing: Pros and cons for computer forensic investigations. *International Journal Multimedia and Image Processing* 1(1/2): 26–34. http://doi.org/10.20533/ijmip.2042.4647.2011.0004

Ridgeway G 2018. Policing in the era of big data. *Annual Review of Criminology* 1: 401–419. https://doi.org/10.1146/annurev-criminol-062217-114209

Sanchez L, Grajeda C, Baggili I & Hall C 2019. A practitioner survey exploring the value of forensic tools, AI, filtering, & safer presentation for investigating child sexual abuse material (CSAM). *Digital Investigation* 29: 124–142. https://doi.org/10.1016/j.diin.2019.04.005

Shah S & Mehtre BM 2015. An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques* 11(1): 27–49. https://doi.org/10.1007/s11416-014-0231-x

Singh S, Jeong YS & Park JH 2016. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications* 75: 200–222. https://doi.org/10.1016/j.jnca.2016.09.002

Standards Australia 2003. *Guidelines for the management of IT evidence*. HB 171-2003. Sydney: Standards Australia International

Strickland C, Kloess JA & Larkin M 2023. An exploration of the personal experiences of digital forensics analysts who work with child sexual abuse material on a daily basis: “You cannot unsee the darker side of life”. *Frontiers in Psychology* 14. https://doi.org/10.3389/fpsyg.2023.1142106

Tabrizchi H & Rafsanjani MK 2020. A survey on security challenges in cloud computing: Issues, threats, and solutions. *Journal of Supercomputing* 76: 9493–9532. https://doi.org/10.1007/s11227-020-03213-1

Tian Y, Tian J & Li N 2020. Cloud reliability and efficiency improvement via failure risk based proactive actions. *Journal of Systems and Software* 163: 110524. https://doi.org/10.1016/j.jss.2020.110524

Torkura KA, Sukmana MI, Cheng F& Meinel C 2021. Continuous auditing and threat detection in multi-cloud infrastructure. *Computers & Security* 102: 102124. https://doi.org/10.1016/j.cose.2020.102124

Victorian Auditor-General’s Office 2018. Police management of property and exhibits. https://www.audit.vic.gov.au/report/police-management-property-and-exhibits

Vistro DM, Rehman AU, Mehmood S, Idrees M & Munawar A 2020. A literature review on security issues in cloud computing: Opportunities and challenges. *Journal of Critical Reviews* 7(10): 1446–1455. https://www.jcreview.com/issue.php?volume=Volume 7 &issue=Issue-10&year=2020

Westlake BG, Brewer R, Swearingen T, Ross A, Patterson S, Michalski D, Hole M, Logos K, Frank R, Bright D & Afana E 2022. Developing automated methods to detect and match face and voice biometrics in child sexual abuse videos. *Trends & issues in crime and criminal justice* no. 648. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78566

Appendix

Table A1: Australian criminal law governing child sexual abuse material

Jurisdiction	Legislation
Commonwealth	ss 474.22–474.24A, *Criminal Code Act 1995* (defences s 474.24)
NSW	ss 91G–91HAA, *Crimes Act 1900* (defences s 91HA(6))
Vic	ss 51B–51H, *Crimes Act 1958* (exceptions 51J(a))
Qld	ss 228A–228DA, *Criminal Code 1899* (exemptions s 228H(1))
WA	ss 217–220, *Criminal Code* (defences and exclusions s 221A(3a))
SA	s 63A, *Criminal Law Consolidation Act 1935* (exemptions s 63C(2a))
Tas	ss 130A–130D, *Criminal Code Act 1924* (defences s 130E(1))
ACT	ss 64–65, *Crimes Act 1900* (no defences or exclusions)
NT	s 125B, *Criminal Code Act 1983* (defences s 125B(2)(a))

Dr Bryce Westlake is an Associate Professor at San Jose State University.

Dr Russell Brewer is an Associate Professor at the University of Adelaide.

Dr Kellie Toole is a Senior Lecturer at the University of Adelaide.

Tom Daly is a Visiting Fellow at the University of Adelaide.

Thomas Swearingen is a Doctoral Candidate at Michigan State University and a Research Associate at the University of Adelaide.

Scott Fletcher is a Cloud Security Specialist at Oracle Corporation.

Franco Ucci is the Senior Director, Cloud Platform Strategy at Oracle Corporation.

Dr Katie Logos is a Lecturer at the University of Adelaide.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website: www.aic.gov.au

ISSN 1836-2206 (Online)   ISBN 978 1 922877 55 0 (Online)

https://doi.org/10.52922/ti77550

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government