INFORMATION SECURITY AND PRIVACY: IS THE AUSTRALIAN GOVERNMENT REALLY PREPARED FOR THE CLOUD?

Akira Takihara Wang
The University of Melbourne
913391

Luke Di Giuseppe
The University of Melbourne
836938

Tate Deklerk
The University of Melbourne
1003713

October 9, 2019

ABSTRACT

Cloud storage is a rapidly developing technology with wide-ranging implications for the way we handle the storage of information. The Australian government is currently in the process of implementing many cloud based services, with intent to expand in the coming years. This paper aims to summarize and critique the current strategies proposed by the Digital Transformation Authority (DTA). We reviewed the most current guidelines, with a focus on information security and privacy, and analysed some of the widely held myths surrounding the emerging technology. We concluded that although cloud storage inherits many complex problems from traditional storage, as well as creating many new ones, it will inevitably improve the efficiency and security of the Australian Government's mass storage solutions. However, some laws and policies followed by the DTA need clarification, and care must be taken to not allow vague guidelines to influence insecure implementation.

1 Introduction

This report outlines the current state of the Australian government's cloud storage strategy, and reviews its methods of implementation. Cloud storage allows the possibility of significant advantages over traditional on-premise storage methods, such as increased scalability, reliability, performance, and more specifiable configurations. [34] However, it introduces a broader range of challenges, both in technical implementation and standard regulation, that must be considered to prevent a range of data loss, data leak and system reliability issues. [19]. These risks pose more serious consequences when considering the sensitivity of the information stored by a government body. This report will identify how the government cloud could potentially affect the privacy and security of Australian citizens, and review the cloud storage implementation strategies of similar governments.

2 Main Requirements of Data Storage

2.1 CIA-triad

For a cloud computing system to reliably store and protect data, it must satisfy a set of criteria that ensures all requirements of successful data storage are met. Traditionally, security requirements for data storage and access are broken down into three main categories: (i) confidentiality, (ii) integrity, and (iii) availability, referred to as the CIA-triad. [24] The term was first coined in 1986 and has since gained popularity amongst information security practitioners [12].

- **Confidentiality** is the prevention of disclosure of information to unauthorised users. Cloud systems must maintain strict confidentiality, as sensitive personal information, such as medical information or criminal records, will be stored on the government data cloud [24]. The consequences of allowing such information to be disclosed to unauthorised personnel can be extremely damaging and can lead to life-threatening situations [36]. Satisfactory confidentiality is achieved through implementing good security protocols, network authentication services and data encryption services, as well as the education of information custodians and end-users [2] [33].

- **Integrity** is the assurance that information remains uncorrupted and complete when being stored and transmitted. Integrity is breached when data is exposed to corruption, damage, destruction, or is otherwise disrupted from its authentic state. [33]. A compromise in information integrity can have a wide range of adverse consequences and can reduce the reliability of a cloud system significantly. [24] For example, a government database may be relied upon by a medical professional to access important patient information in life-threatening situations, where data integrity is a matter of life and death. To prevent integrity loss, hash algorithms and error-correcting codes must be used when transmitting and storing data. Firewall services, communication security and intrusion detection must be used to ensure malicious software is not used to purposefully corrupt data. [2] [33]
- **Availability** is the assurance that data will be accessible to a user or computer system in a timely and uninterrupted fashion. In the case of a cloud storage system, this should apply wherever the data is being accessed. Again, the example of a medical professional needing to access life-saving information quickly highlights the importance of accessibility. Good accessibility is achieved through fault tolerance, authentication systems and security against traffic flow attacks (such as DDoS attacks) [2].

2.2 IAS-Octave

The CIA-triad no longer adequately addresses the risks associated with data storage in a collaborative security environment [24] [12] [33]. Many methods of defining other important requirements of an information storage system exist. Cherdantseva et al. suggests the IAS-octave as a valid extension of the triad, and includes 5 additional requirements.

- **Accountability** is the ability of a system to hold users responsible for their actions [12]. This ensures that a user cannot use, alter or destroy information for a malicious purpose without the system linking them to their action.
- **Auditability** is the ability of a system to conduct persistent monitoring of all human or machine action on the system [12]. This ensures other protocols can be applied in real-time, and the system can handle many access points.
- **Authenticity** is the ability of a system to verify and identify third a third party, and the information it provides [12]. Other requirements, such as confidentiality and integrity, can be breached if there is no trust in third-party information providers.
- **Non-repudiation** is the ability of a system to prove the occurrence/non-occurrence of an event or participation/non-participation of a party in an event[12]. This has implications for a government database, as the legal implications of accessing restricted documents could be severe, and confidence in the system's ability to prove such events is imperative.
- **Privacy** ensures a system obeys privacy policies and enables users to control their personal information [12]. This has interesting implications for a government cloud database, as the personal information of many people will be stored, and they must be allowed to control their data to the extent the relevant privacy laws dictate.

3 Implementation and Deployment

To satisfy the main requirements above, technical implementation and definite security regulations should be established to take advantage of the benefits of a cloud storage strategy.

3.1 Technical Means and Trade-offs

3.1.1 Confidentiality

Encryption is the underlying tool used to provide confidentiality. Beyond that, cloud services provide key management systems (elaborated in section 3.2) and integrated user access management. Various services, such as file storage, web apps and databases are integrated into one cloud. Access of these services are based on the underlying system. This allows easy, centralised management of what services users are granted access to.

3.1.2 Integrity

Integrity of data is mostly contingent on the services that provide availability. Additional measures taken to ensure integrity include Provable Data Posession (PDP) [27]and Proof of Retrievability (PoR) [29] [8]systems. These systems differ in their technical functions, but both provide data integrity across remote servers.

3.1.3 Availability

the Cloud is built upon one main technology: virtualisation. Virtualisation is key in the Cloud's ability to provide availability. It allows a single physical machine to run multiple virtual machines. If a machine fails, another can take up its load without delay. Virtualisation also provides load-balancing, another key capability for availability. This splits the computational load across separate machines, preventing a single machine from being overloaded. The Cloud is also distributed geographically, unlike more traditional data warehouses. This separation is extended to the network as well.

3.1.4 Trade-Offs

- Locking into a vendor: It's easy to migrate to a cloud service, but more difficult to move data and systems out.
- Cost trade-off: If your data storage needs are easy to predict, scalable cloud storage is not worth the price[23].
- Control and governance: Adherence to security policy slows down productions [1]. However, as government agencies are already strictly controlled by strict guidelines, this trade-off mostly applies to businesses.

These trade-offs need to be considered when deciding on the specifics of the Government cloud infrastructure, and different approaches may be needed for different types of data storage.

3.2 Key Management

The efficient management of encryption keys plays a critical role in the security and reliability of a cloud storage system [11]. A key management system (KMS) is needed to direct cryptographic operations between storage providers and data owners. Many complex issues arise surrounding which parties hold an encryption key, and how many layers of encryption are present [37]. The google cloud, for example, offers clients the ability to encrypt their data separately from Google's server side encryption [15]. Several key storage scenarios should be explored, as they offer differing benefits and drawbacks.

3.2.1 Scenario - Data Key Owner: Storage Provider

Data physically resides on the storage infrastructure owned by the storage provider, and so an argument can be made that they, and only they, hold onto encryption keys. This provides several benefits:

- Storage providers will have a more reliable system for key storage and management than clients in many cases, and their protocols can be advertised and critiqued to ensure adequacy.
- The KMS must be run on the server side regardless of where the key is managed, and so less systems are relied upon for fault-free data accessibility.

However, storage providers will almost certainly be the target of attackers aiming to reveal keys, and so the system must ensure that a total leak of all keys is extremely unlikely.

3.2.2 Scenario - Data Key Owner: Data Owner

Allowing (or requiring) the data owner to also provide a key to encrypt their data allows several benefits [22]:

- In the event of a total data breach from the storage provider, the data would still be safe from interpretation unless the client key was separately acquired.
- The client can fulfill their own key security desires as they see fit, and they do not need to rely on the storage provider to keep their policy assurances

The drawback of allowing this additional encryption lies in the unreliability of the client base as a whole. Many clients will be much more at risk of losing access to their key than the service provider, and this could result in data being lost forever.

In the case of a government cloud, this could help keep sensitive data specific to the needs of a particular user. For example, allowing a medical association to control certain keys to access medical data could garner more confidence in the privacy of patient data.

4 Possible Attackers

4.1 Nation States

Nation states attackers have an incentive to collect classified information, including from the Australian government. This classified information can range from personally identifiable information to protected documents. Nation states primarily use

remote attacks, including Advanced Persistent Threats and Denial of Service. Potential attacks from other nation states are complex to handle. Attribution can be difficult, and the consequences for false attribution are dire. Attacks may be tracked to a single country of origin. But even then, it is difficult to distinguish between state actors and other groups operating in that country. The law handles each case differently. They are either a criminal offence or break international law [18]. Even if it is traced to a nation state actor, governments sometimes don't want to attribute it to that state because it could be a sign of aggression. Even if they were to publicly attribute the attack to a sponsored state actor, repercussions could be little to nothing.

4.2 Cyber Criminals

Cybercrime is unique in that it is "any crime that is facilitated or committed using a computer, network, or hardware device" [26]. A cybercrime refers to a singular or discrete event (a data breach may have consisted of many breaches of law) [16]. Cybercrime is primarily done for financial gain. For criminals, cybercrime can be more attractive because it's more discrete than the more traditional physical crimes. It's much easier to attack unknowing victims, and people are inherently less aware of crimes they can't see.

4.3 Disgruntled Employees and Whistleblowers

Disgruntled employees are people who release secret information outside of their organization. They do so to tarnish the reputation of that organization, or to cause them legal or financial harm. As they are already within the organisation, they are well placed to exfiltrate data, but may lack the knowledge to do so. Disgruntled employees don't normally work with outsiders [9].

Whistle-blowers are internal operatives who report a misconduct case to an external body [25]. They are motivated by both personal and interpersonal factors i.e. their own integrity and concerns for public safety [35]. Sometimes, they work with outsiders to perform their attacks. A well-known example of this is when Julian Assange assisted Chelsea Manning [31].

5 Attack Scenarios

5.1 Distributed Denial of Services Attack (DDoS)

A DDoS attack involves flooding the target with large amounts of traffic. Against Cloud infrastructure, SNMP attacks have been popular [10]. These attacks utilise bot-nets –large groups of interconnected computers. As such, only well-funded nation states or criminal organisations conduct these attacks. Protections against these attacks are provided by the cloud service providers – at an extra cost.

5.2 Social Engineering for Password Stealing

Social engineering exploits the weakest component of any technical system: the human element. The term social engineering incorporates various methods, including phishing and physical attacks. All endpoints that have access to the Cloud need to be protected. Remote phishing attacks against personnel are likely to be conducted. These attacks could successfully install key-loggers on end devices to steal that user's credentials. Internal actors could use established trust to gain access to passwords. Shoulder surfing or dumpster diving can be performed [21].

A protection against this would be a Multi-Factor Authentication system. It would require a user to input their password plus a one-time password. The one-time password is provided via an additional device –either software or hardware.

5.3 Web Injection

An injection vulnerability allows an attacker to, through a web-facing application, execute code that should not executed [17]. These are types of remote attacks. If vulnerabilities are unknown, then the issues can go un-addressed for months – even years. Luckily, the Cloud enables DevOps [7], which then enable secure coding practices (through package management and scanning). While not a fail-safe, it can help mitigate vulnerabilities.

6 DTA Secure Cloud Strategy and Open Questions Regarding the Cloud

Digital Transformation Authority (DTA) is in charge of developing strategies and training agencies to implement cloud storage. Although there are many recognised benefits to using the Cloud, there are valid arguments against its immediate implementation in the Government sector:

- The Cloud is not as secure as on-premise services.

- Privacy policy prevents government data residing offshore.
- Information in the Cloud is not managed properly and does not comply with record-keeping obligations

The Australian Signals Directorate (ASD) Certified Cloud Services provides a list of providers [14] that can allow up to *PROTECTED data to be stored off-shore. In Summary, cloud storage for defence secrets and top-level government data have yet to be addressed, and will not follow migration until the basic cloud is implemented across lower-level agencies.

Several open questions exist regarding the implementation of cloud storage, and they must be properly addressed before a reliance on cloud is to be accepted.

6.1 Is on-site storage more secure than the Cloud?

6.1.1 Supporting Arguments

Although cloud storage may not seem as secure as an on-site database, the majority of its security risks are equally applicable to an on-site database. If anything, cloud service providers will have dedicated teams to monitor and prevent security attacks, whereas an on-site database is limited to the few employees that manage the database. It can also be argued that on-site database models allow the government to control access to its data (such as local access only). In theory, this may be true, but there have been several cases [30], [28] where security breaches have resulted due to some malicious intention of an employee. Examples of such breaches include: a Network Engineer at EnerVest which sabotaged and reset the database resulting in a loss of USD$1 million [20], a Tesla employee stole and sold 50TB of sensitive data [32] and Documents from LandMark White (an upcoming Australian bank) were sabotaged by an unnamed employee [6]. Breaches that occur this way can take a significant time to discover and handle because there is no dedicated team to do such a job.

6.1.2 Arguments Against

In conjunction, cloud models require high investment up-front, with no return until a significantly later time. Furthermore, cloud technology is not created by the government but rather obtained via third party private companies. This may raise concerns and potential conflicts of interest if the third party is malicious, even if they have been certified by the ASD [14]. A service provider can access the data stored on the Cloud at any time given they have the decryption key. They may observe and control access traffic and configure firewalls maliciously to allow vulnerabilities and backups created by the service provider may be accessed without the data owner knowing. The lack of transparency can make it difficult for a government body to trust the cloud provider with sensitive data

6.1.3 DTA Strategy Argument

The DTA contends that the strong security risk management with cloud storage outweighs its risks. This is due to the automation in place which minimises human error which may otherwise cause security risks in on-site database centres. Furthermore, the DTA suggests that because cloud service providers base their reputation on being secure, they will often implement and manage significantly better security controls than on-site database centre teams. At the same time, the DTA also claims that on-site data centres are open to the same types of attacks as a cloud based system, simply due to their connection to the internet.

It must also be noted that cloud models and on-site databases can still suffer from a social-engineering attack. On-site databases may be more secure in the sense that all employees require background checks (more-so if it is a government agency), but it can also be easily thwarted if the data is stored in the Cloud in an unknown location.

It may be worthwhile for the government to implement and migrate non-sensitive data to the Cloud to test if it is indeed better. Although the investment may be costly, cloud storage can be up-scaled flexibly allowing for a full migration without any hassle. Despite the downside of having little visibility and transparency in the process, the DTA has suggested that agencies develop their cloud strategy which adheres to their purpose, allowing full control and planning at every step during migration to the Cloud. These findings by the DTA are in line with the findings of other research, and appear sound.

6.2 Can Government Data Legally Reside Offshore?

6.2.1 Supporting Arguments

There is a whole policy in place [5], which enforcers an entity to adhere to the correct standards when outsourcing its data off-shore. Likewise, a Cloud Services Panel (CSP) and certification via the ASD has been in operation to enable government agencies to request quotes for services and obtain certification and accreditation statuses.

By law, the 8th Australian Privacy Principle (APP) provides criteria for off-shore storage of personal information. This has made government agencies and cloud service providers accountable for preserving confidence in data being stored off-shore.

6.2.2 Arguments Against

Data sovereignty is often the main barrier for the government cloud. Many government agencies will remain unwilling to store their data off-shore. In 2014, the Australian Government experienced such an issue:

> "Australia has cancelled a government contract with a cloud service provider when it was discovered that the Italian company used an off-shore cloud to process its data. Specifically, it was revealed that up to 80,000 ADF personnel data was sent overseas since 2012" [13].

Even if data is hosted within a distributed cloud, the service provider may not store the data in locations obvious to the data owner. Advocates for the privacy of government data strongly suggest that an on-site database premise with sufficient security risk management will outweigh the benefits of the Cloud. In practice, all Defence Secrets and Top-Level Government Data will remain on-site [14], so this implies that on-site storage of data is still considered to be more secure. In parallel, a downside of having off-shore cloud storage is that the control of data is reduced.

6.2.3 DTA Strategy Argument

Although there are many sound arguments against storing data off-shore, the DTA proposes a new initiative to redevelop the CSP to better align agencies to enable cloud commodity purchases. The APP and Privacy Act in place also have clear guidelines regarding access and storage of personal information. However, there is a questionable policy by the AIC which states that an entity must have *reasonable steps* to ensure the protection of personal information. Yet, the *reasonable steps* are quite vague and ambiguous which may lead to loopholes in the system. But, the ASD provides a certified list of Cloud service providers all of which are allies of Australia (such as the USA), and have already on agreed on some sharing of defence secrets and sensitive data [4]. Because of this, the list provides an excellent source of Cloud providers with an already strong mutual trust. These findings by the DTA are sound, and comparing them to previous research, they appear sound.

6.3 Does good privacy practice imply that off-shore storage is risky or stupid?

6.3.1 Supporting Arguments

Current practices within the Australian government limit all data stored in the Cloud to be at most PROTECTED* class, storing more classified documents on-site [14].This implies that current privacy policy points to on-site storage as the more secure storage option. Indeed, many other sources agree on this point [4] [13].

6.3.2 Arguments Against

In theory, if the Australian government is unable to trust its allying countries to store its data, then it may imply that we do not fully trust them as allies. From the list of certified cloud service providers [14], almost all providers are American based - the strongest ally Australia has. One may also argue that the insecurity of data does not signify the insecurity of information. With good privacy practices such as strong encryption, storing data off-shore should not compromise information security.

6.3.3 DTA Strategy Argument

The Privacy Act in Australian law states that it does not prevent an entity from utilising a cloud service provider to store or process personal information off-shore. Rather, it is stated that the entity itself has to comply with the APPs and is held accountable for the querying of data to off-shore Cloud service providers. The DTA also argues that the Australian Information Commissioner's (AIC) guide requires *reasonable steps* to be in place to ensure the protection of personal information. Furthermore, The DTA argues that the APP frameworks [5] have established all accountabilities to ensure that suitable privacy and security controls are developed to preserve confidence in the personal data being stored in the Cloud.

The vague nature of these policies is alarming - a sentiment supported by findings by the Discovery Research Feedback [3] which revealed that government agencies were not content with the current policies in place. It also contended current privacy practices in on-shore databases outweighed off-shore cloud storage. Hence, the DTA's policy in this area needs revision give confidence in objectively secure off-shore storage.

7 Conclusion

Although cloud technology is certainly powerful and cost efficient, it inevitably inherits the original problems of current on-site database models with additional obstacles such as data sovereignty. The DTA Secure Cloud Strategy makes sound arguments and suggests numerous solutions to these obstacles, but further research yielded agencies not being content with the current policies in place.

Future suggestions for policies include (but not limited to) more precise guidelines and definitions of privacy, as well as a revision of the AIC policy. Notably, the *reasonable steps* specified are vague and can hold several interpretations, so it is unclear whether or not an entity or private cloud service provider will be held accountable when there is a breach or compromise in data.

References

[1] *A CIO's guide to the cloud: hybrid and human solutions to avoid trade-offs | Google Cloud Blog*. URL: https://cloud.google.com/blog/topics/hybrid-cloud/a-cios-guide-to-the-cloud-hybrid-and-human-solutions-to-avoid-trade-offs.

[2] Ashish Agarwal and Aparna Agarwal. "The security risks associated with cloud computing". In: *International Journal of Computer Applications in Engineering Sciences* 1 (2011), pp. 257–259.

[3] Digital Transformation Agency. *Secure Cloud Strategy*. 2017. URL: https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/cloud/secure-cloud-strategy.pdf.

[4] BUREAU OF EAST ASIAN and U.S. Department of State PACIFIC AFFAIRS. *U.S. Relations With Australia*. Aug. 2018. URL: https://www.state.gov/u-s-relations-with-australia/.

[5] Office of the Australian Information Commissioner. *Australian Privacy Principles*. Aug. 2019. URL: https://www.oaic.gov.au/privacy/australian-privacy-principles/.

[6] Julian Bajkowski. *LandMark White says new SCRIBD leak is sabotage*. May 2019. URL: https://www.itnews.com.au/news/landmark-white-says-new-scribd-leak-is-sabotage-525984.

[7] Armin Balalaie, Abbas Heydarnoori, and Pooyan Jamshidi. "Microservices architecture enables devops: Migration to a cloud-native architecture". In: *Ieee Software* 33.3 (2016), pp. 42–52.

[8] Kevin D Bowers, Ari Juels, and Alina Oprea. "HAIL: A high-availability and integrity layer for cloud storage". In: *Proceedings of the 16th ACM conference on Computer and communications security*. ACM. 2009, pp. 187–198.

[9] Alvaro Cardenas et al. "Challenges for securing cyber physical systems". In: *Workshop on future directions in cyber-physical systems security*. Vol. 5. 1. 2009.

[10] Andrew Carlin, Mohammad Hammoudeh, and Omar Aldabbas. "Defence for distributed denial of service attacks in cloud computing". In: *Procedia computer science* 73 (2015), pp. 490–497.

[11] Ramaswamy Chandramouli, Michaela Iorga, and Santosh Chokhani. "Cryptographic key management issues and challenges in cloud services". In: *Secure Cloud Computing*. Springer, 2014, pp. 1–30.

[12] Yulia Cherdantseva and Jeremy Hilton. "A reference model of information assurance & security". In: *2013 International Conference on Availability, Reliability and Security*. IEEE. 2013, pp. 546–555.

[13] Paris Cowan. *Defence contractor ditched over data offshoring*. July 2014. URL: https://www.itnews.com.au/news/defence-contractor-ditched-over-data-offshoring-390379.

[14] Australian Signals Directorate. *ASD Certified Cloud Services*. Oct. 2019. URL: https://www.cyber.gov.au/irap/asd-certified-cloud-services.

[15] Google. *Customer-managed encryption keys*. Sept. 2019. URL: https://cloud.google.com/storage/docs/encryption/customer-managed-keys.

[16] Sarah Gordon and Richard Ford. "On the definition and classification of cybercrime". In: *Journal in Computer Virology* 2.1 (2006), pp. 13–20.

[17] Bernd Grobauer, Tobias Walloschek, and Elmar Stocker. "Understanding cloud computing vulnerabilities". In: *IEEE Security & privacy* 9.2 (2010), pp. 50–57.

[18] Clement Guitton and Elaine Korzak. "The sophistication criterion for attribution: Identifying the perpetrators of cyber-attacks". In: *The RUSI Journal* 158.4 (2013), pp. 62–68.

[19] Ibrahim Abaker Targio Hashem et al. "The rise of "big data" on cloud computing: Review and open research issues". In: *Information systems* 47 (2015), pp. 98–115.

[20] Chris Kanaracus. *Ex-network Engineer Faces Prison After Admitting He Sabotaged Employer's System*. Jan. 2014. URL: https://www.cio.com/article/2379122/ex-network-engineer-faces-prison-after-admitting-he-sabotaged-employer-s-system.html.

[21] Katharina Krombholz et al. "Advanced social engineering attacks". In: *Journal of Information Security and applications* 22 (2015), pp. 113–122.

[22] Witold Litwin, Sushil Jajodia, and Thomas Schwarz. "Privacy of data outsourced to a cloud for selected readers through client-side encryption". In: *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM. 2011, pp. 171–176.

[23] 2017 March 8. *Is the Cloud Right for You? The Trade-Offs of Cloud Computing*. Mar. 2017. URL: https://www.channelfutures.com/cloud-2/is-the-cloud-right-for-you-the-trade-offs-of-cloud-computing.

[24] A. Mosenia and N. K. Jha. "A Comprehensive Study of Security of Internet-of-Things". In: *IEEE Transactions on Emerging Topics in Computing* 5.4 (Oct. 2017), pp. 586–602. DOI: 10.1109/TETC.2016.2606384.

[25] Janet P Near and Marcia P Miceli. "Organizational dissidence: The case of whistle-blowing". In: *Journal of business ethics* 4.1 (1985), pp. 1–16.

[26] Donn B Parker. *Fighting computer crime*. Scribner New York, NY, 1983.

[27] Sunita Sharma. *Data Integrity Challenges in Cloud Computing*. Mar. 2016. URL: https://pdfs.semanticscholar.org/2760/46ac1e0fa92763a1444a8097bf81a79a54f9.pdf.

[28] Buckley Smith. *Laying blame on employee in Desjardins data breach is ignoring the big picture, security experts say*. June 2019. URL: https://www.itworldcanada.com/article/laying-blame-on-employee-in-desjardins-data-breach-is-ignoring-the-big-picture-security-experts-says/419299.

[29] Emil Stefanov et al. "Iris: A scalable cloud file system with efficient integrity checks". In: *Proceedings of the 28th Annual Computer Security Applications Conference*. ACM. 2012, pp. 229–238.

[30] Steve Turner. *2019 Data Breaches - The Worst So Far*. Oct. 2019. URL: https://www.identityforce.com/blog/2019-data-breaches.

[31] *United States of America v Julian Paul Assange*. 17-MJ-611. Dec. 21, 2017. URL: https://www.documentcloud.org/documents/5913205-Assange-Affidavit.html.

[32] Jai Vijayan. *Tesla Employee Steals, Sabotages Company Data*. June 2018. URL: https://www.darkreading.com/informationweek-home/tesla-employee-steals-sabotages-company-data/d/d-id/1332098.

[33] Michael E Whitman and Herbert J Mattord. *Principles of information security*. Cengage Learning, 2011.

[34] Jiyi Wu et al. "Cloud storage as the infrastructure of cloud computing". In: *2010 International Conference on Intelligent Computing and Cognitive Informatics*. IEEE. 2010, pp. 380–383.

[35] Peter Yeoh. "Whistleblowing: motivations, corporate self-regulation, and the law". In: *International Journal of Law and Management* 56.6 (2014), pp. 459–474.

[36] Meng Zhang, Anand Raghunathan, and Niraj K Jha. "Trustworthiness of medical devices and body area networks". In: *Proceedings of the IEEE* 102.8 (2014), pp. 1174–1188.

[37] Gansen Zhao et al. "Trusted data sharing over untrusted cloud storage providers". In: *2nd IEEE International Conference on Cloud Computing Technology and Science*. IEEE. 2010, pp. 97–103.