Cyber Concerns With Cloud Computing

Jacob Chan and Mark Reith
Air Force Institute of Technology, Dayton OH, United States
jacob.chan@afit.edu
mark.reith@afit.edu

Abstract: The last two decades has seen a paradigm shift towards cloud-based services, cloud-central storage, and cloud computing. The benefits of this shift has been undeniable, including minimal user infrastructure needed to achieve what appears to be limitless data storage, powerful processing capabilities, and services that scale according to demand. However, when there is an upside there usually exists a downside. Cloud computing brings many security and cyber concerns that stems from the inherent insecurity of having large concentrations of data and assets in the cloud, making it a priority target for malicious actors. This survey paper will provide a review of the existing cyber concerns with cloud computing from a military perspective and point out future cyber concerns that may populate due to emerging technological advancements on the horizon.

Keywords: cloud computing, cloud-based services, cloud solutions, cloud computing security, cloud security concerns

1. Introduction

The continued paradigm shift in the last two decades towards cloud-based services and cloud storage solutions has provided not only a myriad of benefits for companies and individuals alike but has unveiled cyber concerns that stems from the inherent insecurity of having large concentrations of data and assets in the cloud, making it a priority target for malicious actors. This survey paper will provide a review of the existing cyber concerns with cloud computing that have been identified insofar from a military perspective and point out future cyber concerns that may populate due to emerging technological advancements on the horizon. To prepare readers in understanding relevant cyber concerns with cloud computing, this paper first provides background context on what cloud computing is, types of clouds and service models, and the benefits of cloud computing. Next, the paper goes into the depths of various cyber concerns related to cloud computing, ranging from confidentiality/privacy issues to insider threats, before highlighting potential cyber concerns for the future.

1.1 What is cloud computing?

The fundamental concept of cloud computing can be generalized to centralizing data storage, applications, and computing capacity to the network core (the Cloud) and providing end-user access to the Cloud as a service (Hayes, 2008). The idea of the Cloud is not a novel one and has been conceptualized as early as the 1950s, in the form of time-sharing systems (Earnest, 2016). During that time, computers were large mainframes that required an entire room to store and an equally large amount of power and electricity to host. The benefits provided by a mainframe were undeniable but not everyone had the money or room for one. Time-sharing systems connected smaller user terminals to mainframes and allowed people to leverage the benefits of computers without physical access to a mainframe, which was a predecessor to the client-server architecture of today. By the 1980s, personal computers had their own storage capacity and provided an array of applications that could be personalized to the individual user, making personal computers the ideal choice for computing and storage needs. In the past two decades, the tides of computing have once again shifted, with the increasing demand for digital storage and processing power for both individuals and organizations alike pushing the responsibilities and capabilities of digital storage and computing into the Cloud (Hayes, 2008). In particular, the Cloud offers an intriguing outlook for the U.S. military's growing demand for technological solutions (the U.S. was the country with the second highest R&D spending in 2021) (Szmigiera, 2021).

1.2 Three types of clouds

- 1) Public Clouds: The most common and vulnerable type of cloud are public clouds (Almorsy, Grundy and Müller, 2016). They include the free or paid cloud services and resources offered to the public. Companies that offer public clouds include Google, Amazon, Microsoft, IBM, Oracle, and more. Just as normal civilians do, U.S. military service members utilize public cloud services such as Google Docs or Dropbox all the time, in both their personal lives and at work.
- 2) Private Clouds: Private cloud resources and services are usually not free, and a private cloud is only accessible to private organizations or businesses that have permissions to access that specific cloud

(Srivastava and Khan, 2018). It is worthy to note that a public cloud provider can also offer private cloud services, through virtual partitioning of their cloud (Armbrust, 2010). An example is the Commercial Cloud Services (C2S) contract that the U.S. Intelligence Community (IC) has had with the one of the leading public cloud providers of the world, Amazon Web Services (AWS) since 2013 (Miller, 2021). Part of this $600 million contract is that AWS must service the private cloud needs of intelligence organizations such as the CIA, the FBI, and the NSA. In 2017, Amazon came out with the AWS Secret Region, which offers cloud services and storage for U.S. secret-level data and follows "the Director of National Intelligence (DNI) Intelligence Community Directive (ICD 503) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4" (AWS Public Sector Blog Team, 2017). AWS Secret Region is offered to the U.S. IC as part of the C2S contract but non-IC U.S. government customers with secret-level clearance may also utilize AWS Secret Region with the proper contracts.

- 3) Hybrid Clouds: Hybrid clouds are a combination of multiple clouds, which can include public and private clouds (Srivastava and Khan, 2018). These types of clouds have become increasingly popular in the last couple years as cloud providers have become more competitive, with some offering distinct services. For example, in 2020, the U.S. IC awarded their Commercial Cloud Enterprise (C2E) contract to five different cloud providers: AWS, Microsoft, Google, IBM, and Oracle (Moss, 2020). The C2E contract, estimated to be worth north of $10 billion allows the IC to select among the five cloud providers that best fulfills their cloud needs. Back in July of this year, the DoD cancelled their Joint Enterprise Defense Infrastructure (JEDI) contract, worth $10 billion over 10 years with Microsoft in favor of the Joint Warfighting Cloud Capability (JWCC) contract, which seeks solutions from multiple cloud vendors (Feiner, 2021). According to an official statement released by the DoD, the JWCC contract will better fulfill the DoD's increasing need for cloud capabilities as posed by newer requirements such as the Joint All Domain Command and Control (JADC2) and the Artificial Intelligence and Data Acceleration (ADA) initiatives (Department of Defense, 2021).

1.3 Cloud service models

Cloud computing goes by many different names such as utility computing, on-demand computing, Software-as-a-Service (SaaS), internet as a platform, and many others (Hayes, 2008). Regardless of the name, most forms of cloud computing usually offer the following services.

- 1) Software as a Service (Saas): SaaS provides rich and practical applications to users that are easily accessible through a web browser without needing to install, update, and maintain software on their own personal computer (Srivastava and Khan, 2018). Examples of this include Google Workspace, which encompasses Google Docs, Google Spreadsheets, Google Drive, and Office 365, which boasts the entire Microsoft Office suite, all easily accessible online. As mentioned before, military service members use these cloud applications all the time. There are no specific regulations on cloud application usage for individual service members in the military. Instead, their usage is governed through the individual branch's regulations on information systems usage and classification guides.
- 2) Platform as a Service (PaaS): PaaS gives individual users and organizations an existing digital platform and frameworks to develop and customize applications, manage their business, or to carry out organizational functions irrespective of their own hardware setup (Srivastava and Khan, 2018). An example of this is Platform One, which is a secure DoD cloud platform that provides developers with existing tools, software, frameworks, and DevSecOps pipelines that allow them to solve complex problems using a 90% ready software solution from day one instead of starting from the ground up (Office of the Chief Software Officer, 2021). Simply put, Platform One allows DoD developers to focus on developing software solutions without having to worry about building a platform to develop software solutions.
- 3) Infrastructure as a Service (IaaS): IaaS refers to the physical and digital infrastructure needed to enable SaaS and PaaS on demand (Srivastava and Khan, 2018). This includes the servers, server racks, data centers, operating systems, communication hardware, and everything provided by cloud providers that cloud users interact with daily but never get to see. With IaaS, cloud customers do not need to set up their own infrastructure and can instead, rely on the existing infrastructure set up by the cloud provider. In 2010, the DoD started the Federal Data Center Consolidation Initiative (FDCCI) with goals of reducing the number of DoD-operated data centers by 60% by the end of 2018 (DoD Inspector General, 2016). The purpose was to save on costs associated with acquisition, sustainment, and manpower, reduce the DoD's real-estate and digital footprint which in turn reduces cyber-connected attack surfaces, and focus resources on necessary

war-fighting capability. Since 2016, the DoD has saved almost $2 billion from closing 210 tiered data centers and 3005 non-tiered data centers (Office of the Federal Chief Information Officer, 2021).

1.4 Benefits of cloud computing

The list of benefits for cloud computing is long and ever-growing. This paper will not extensively list all the benefits of cloud computing but will rather focus on the ones that will line the talk for cyber concerns mentioned later in the paper.

- 1) Minimal User Infrastructure: One of the biggest benefits about cloud computing that captivates customers is that there is minimal user infrastructure required. Cloud service providers supply the hardware and software infrastructure necessary for cloud applications, storage, and computing. Businesses and organizations can leverage this existing infrastructure for their own use and can save on costs of purchasing servers and setting up server racks, purchasing or renting space to host said servers, buying and configuring operating systems and server-side security such as antivirus, firewalls, or intrusion detection systems (IDS), and hiring/training employees to use, maintain, and upgrade this infrastructure. As mentioned previously, part of the DoD Cloud Strategy is to consolidate data centers and drive IT reform at the DoD (Department of Defense, 2018). By reducing unneeded infrastructure, the DoD hopes to reduce security risks/attack surface and redirect resources to war-fighters and workforces from different mission areas. Aligned with this initiative is the $62 million Private Cloud II contract that the U.S. Army awarded to IBM in 2016 (Serbu, 2016). The agreement states that IBM must set up, maintain, and operate a data center in Redstone Arsenal, an army post near Huntsville, Alabama, serving as a pilot initiative for a private company to operate a data center on U.S. military installation grounds. Although the Army added a data center through the contract, it is part of the consolidation effort to remove unnecessary data centers and push data center management responsibilities to private companies.
- 2) Amortized Spending: With cloud computing, there is no big upfront cost associated with purchasing expensive equipment and software (Almorsy, Grundy and Müller, 2016). Instead, there is an amortized cost in which cloud customers pay monthly (there exist options for yearly payments) based off how much computing power they used, the amount of storage they required, the type of services they needed, etc. This is especially relevant to the DoD, because a lot of organizations within the DoD are allotted funds per year. Some Air Force squadrons, or wings will spend the rest of their funds toward the end of the year because they may lose it if they don't use it, or it may affect how much they are allocated the following year. With cloud computing, spending is more streamlined and efficient because organizations are spending funds based off their usage and needs, which may change throughout the year as opposed to end-of-year spending to avoid wasting funds. It is important to note that while most military cloud utilization instances mentioned so far have been large ventures on the DoD (JWCC) or department level (Army Private Cloud II), smaller organizations such as Air Force squadron or wings can still utilize cloud computing and reap the benefits from amortized spending.
- 3) Elasticity: As mentioned just now, cloud computing provides customers with a flexibility in spending based off evolving needs, commonly referred to as elasticity. With elasticity, cloud customers are protected from over or under-provisioning (Armbrust, 2010). Businesses and organizations tend to provision service requirements according to peak hours. This may result in an over-provisioning of resources. For example, if the Air Force portal experiences peak hours at noon on Mondays and Fridays, the Air Force may add extra servers to meet that peak demand. However, the extra servers are idle and wasted during non-peak hours (which in this case, is most of the week). On the flip side, under-provisioning can be just as problematic. Imagine in the previous example that the Air Force decides to provision just enough resources to handle normal usage. There is an unexpected event (i.e., COVID-19 or a natural disaster) and the Air Force portal is receiving an influx in activity. In this instance, it is paramount for the Air Force to increase resources to meet demand. However, this demand may soon die down and the Air Force is left with even more wasted resources. Cloud computing offers a flexible and scalable solution for businesses and organizations to meet elastic and changing demands (Zissis and Lekkas, 2012). Amazon Web Services (AWS) allows customers to "pay as you go" (Bishe, 2018). They can pay for storage by the gigabyte and processing power by the hour, allowing businesses and organizations to scale up during peak-hours and scale back down afterwards.

1.5 Prior cloud security research

Chen, Paxson and Katz (2010) attempts to separate security problems unique to cloud computing from the legacy security problems that existed since the development of time-sharing systems. The authors argue that most cloud security concerns are not new but rather variations of historical web application problems. There are, however, two new security concerns specific to and brought on by cloud computing: multi-party trust considerations and mutual auditability. Trust considerations are different for the cloud because multiple parties are sharing resources. In particular, concerns exist with cloud customers being able to view each other's activity, businesses accessing proprietary data from their competition (cloud providers can also be the ones accessing competitive data), or cloud customers using the Cloud to run botnets, spam campaigns, or password brute-forcers. These issues result in the need of mutual auditability between cloud customers and cloud providers. Zissis and Lekkas (2012) examines unique security requirements related to the cloud and proposes a solution using a Trusted Third Party alongside Public Key Infrastructure (PKI) to ensure confidentiality, integrity, and authenticity of data. They highlight the notion of trust in traditional computing, which is based on security policy vs. cloud computing, in which users have to trust the processes and security set in place by the cloud provider. Furthermore, trust is delegated to cloud providers in public clouds while trust remains within the organization for a private cloud. The authors proposes a trusted authority (Trusted Third Party) that addresses security concerns within the cloud and facilitating trust between cloud providers and cloud customers. Almorsy, Grundy and Müller (2016) explores the cloud security problem from multiple perspectives including the cloud stakeholder's perspective, the architecture-level perspective, cloud characteristics perspective, and cloud service model delivery perspective. Cloud stakeholders include cloud providers, service providers to deliver content and services using the Cloud, and service users. Each stakeholder has different security needs and expectations. The authors propose service-level agreements (SLAs) and security transparency as a solution to resolve such conflicts. They divide cloud issues into subsections related to the different SaaS, PaaS, and IaaS service models and provides a cloud computing dependencies stack containing VMs, APIs, Services and Applications that the cloud service models rely on, which reveals vulnerabilities inherent in the cloud architecture. While the aforementioned authors do a great job highlighting cloud-related security issues, they do not touch upon the issues from a military perspective. Cloud issues may have differing levels of effects, likelihood, and tolerance for the military than civilian customers. For example, it can be argued that most if not all cloud customers likely value mutual trust with cloud providers. From the perspective of the military, trust may be the single most important requirement within cloud computing and a lack of data confidentiality is often intolerable (i.e. recent discussions on supply chain security). While many cloud customers, especially big companies, also have a lot to lose in the event of a data breach, it usually does not affect national security. Military and defense contractor customers often deal with classified data, which may bring upon unique issues or require specialized solutions, and it may be valuable to consider cloud security from their perspective. Ďulík (2016) looks at the benefits cloud computing can provide to the military and potential risks the military should consider. The author considers private clouds to be most appropriate for the military and highlights the different security mechanisms provided by the private cloud reference model. The author does a great job explaining the benefits, risks, and security issues special to the military at the time but does not look at how upcoming technology can impact cloud security for the military.

2. Cyber concerns

While many advantages of cloud computing come from centralizing data and services within the Cloud, it is also this inherent concentration of data and assets that brings about cyber concerns in the first place. Although, it is true that some of the security concerns seen in cloud computing can also be related back to traditional decentralized computing, this paper will not compare the security concerns of cloud computing and traditional computing, nor will it assume on which is more secure. Whether the Cloud is perceived to be secure or not, it will, no doubt, continue to proliferate and be used globally. The number of internet users utilizing some type of cloud service has grown from 2.4 billion in 2013 to 3.6 billion in 2018 (Statista, 2014). Since the Cloud will continue to grow regardless, it is best to focus our attention on security issues with cloud computing and hopefully spark some innovative solutions to fix them.

2.1 Centralized target

The top three industries targeted by cyber espionage in 2020 were finance, information, and healthcare. Cloud computing makes it easier for malicious actors by congregating the data and operations of multiple sectors in one place, making the Cloud a centralized target. Beyond that, cloud computing generated over $300 billion

dollars of revenue in 2020. This makes cloud providers themselves an attractive target for cyber espionage, ransomware, denial-of-service attacks, phishing attempts, and more. With the emergence of private clouds for the military and the DoD's increasing reliance on cloud services, the Cloud has become a viable attack vector for both state and non-state adversaries that hope to steal sensitive data from the U.S. government.

2.2 Single-point-of-failure

Beyond client-side systems and the actual data, everything else in cloud computing are provided by cloud providers including servers, buildings that house the servers, software, data storage, processors, and services. This makes the Cloud, a single-point-of-failure. It can be argued that most cloud providers, being multi-billion-dollar businesses, have redundancy built-in such as multiple data centers, emergency power, backup storage, etc. However, their redundant systems and infrastructure could be vulnerable to the same attacks or issues that caused the original systems to go down if they use similar software, servers, or if their infrastructure is set up the same way (Armbrust, 2010). Some events also cannot be planned, such as if the cloud provider goes out of business. If a cloud provider goes out of business or gets knocked off the net, can a customer's data be transferred to another cloud provider? Can it be transferred in time before the original cloud provider's systems get decommissioned? If the cloud goes down, can businesses or organizations still function, or will they have to shut down? These questions are especially concerning for the military because the military is responsible for a wide array of critical functions including national security. If the cloud goes down, the military cannot simply go home for the day. Thus, the DoD is especially concerned with redundancy and recovery options that exist with cloud computing. One solution to the single-point-of-failure problem is to utilize multiple cloud providers, but the downside is that there may be hefty additional costs associated with maintaining the same instances of data and applications with multiple vendors. The DoD is headed towards this direction of leveraging multiple cloud providers as evident in the 2018 DoD Cloud Strategy and the JWCC contract (Department of Defense, 2018).

2.3 Insider threat

A lot of security concerns are focused on the security of the Cloud and how to prevent intruders from getting in. Other threats come from within the Cloud. In the Trojan War, instead of breaking into the impenetrable walls of Troy, the Greeks decided to hide in the Trojan Horse and win the war from the inside. In the story of cloud computing, Troy represents cloud providers such as Amazon, Google, or Facebook and the Greeks can be anybody. Of course, any business or organization can be a target of an insider threat, but this threat is amplified for cloud providers because of the value of the data contained within the Cloud and the fact that attacking the Cloud is like an attack on thousands of valuable business or organizations simultaneously. Part of this problem can be mitigated by using application-level encryption as an added layer of security (Zissis and Lekkas, 2012). However, the threat posed to the Cloud isn't an insider breaking through encryption as much as the insider gaining access to this information. There exist tools that can break through encryption but there is no tool that can gather the encrypted data of thousands of valuable companies in one place. Correction, the Cloud is that tool. On the government side, military and government private clouds often contain sensitive information that may have ties to national security, policy, and objectives. Some of this information could be classified as well as seen in the C2S and Army Private Cloud II contract. From a DoD perspective, it is paramount for cloud providers that service government needs to have insider threat training for employees, an intensive background check and classification process for new employees and re-evaluations every few years, information sharing guidelines based off need-to-know, detailed logs of employee actions and regular auditing of logs, strong authentication and access control to the Cloud, heavy encryption of customer data that is not readable by employees, and limitation of employee or administrator power.

2.4 Confidentiality/privacy

It is common practice for cloud providers to service multiple clients using the same physical systems and storage devices (Almorsy, Grundy and Müller, 2016). This type of service model can be vulnerable to data spillage, which can result in catastrophic damage to confidential or proprietary information. According to Statista.com, most data stored in the Cloud is considered sensitive data. Likewise, military and government clouds contain sensitive and classified data. Military service members can also accidentally store sensitive data on public clouds. Once again, the DoD is concerned with whether the cloud provider has systems to place to prevent employees and other customers from accessing government data. A partial solution to this problem could be having cloud providers operate private data centers solely for government use as seen in the Army's Private Cloud II contract

with IBM. The latter concern would have to be fixed through stricter and more definitive guidelines on service member usage of the Cloud.

2.5 Availability

Availability of data or service is important in almost any internet-based application, but is scaled up for the Cloud because more customers can be affected by loss of availability. An investment firm could lose millions of dollars if they lost access to proprietary market data that allowed them to move in or out of stocks at a moment's notice. A patient's life could be at risk if a hospital loss access to the Cloud that they used to store patient data. To be fair, a lot of this important data is typically stored locally too but as the Cloud continues to grow in size and application, the consequences of availability issues could grow exponentially. As mentioned before, the military is responsible for national security and numerous missions that span the globe. A lack of availability for military clouds could have a detrimental effect to national security, the economy, diplomacy, and policy, and much more. Using multiple cloud providers certainly helps because it less likely for multiple cloud providers to be unavailable at the same time. However, it is important for the DoD and cloud providers to have disaster recovery plans, continuity of operations procedures, and redundant non-cloud systems in place to mitigate loss of cloud availability.

3. Future cyber concerns

Gordon Moore, the co-founder of Intel stated in 1965 that the number of transistors on a circuit will double every two years, hence doubling computing power every two years. Although the effects of Moore's Law have diminished in the past few years, technological advancements have continued to emerge and will likely continue to prosper for the foreseeable future. Some of these technologies may benefit cloud computing while others may create concerns associated with cloud computing. This section will highlight some of these concerns.

3.1 Quantum computing

Quantum computing is often touted as the next big thing in computers, with the common belief that a sophisticated quantum computer could solve traditional computer problems in a fraction of the time. In theory, RSA encryption using a 2048-bit key would take trillions of years to break using traditional computers (Baumhof, 2019). A quantum computer with 4099 perfectly stable qubits (quantum bits) would break the same algorithm in about 10 seconds. Current quantum technology is still quite a bit off from reaching 4099 qubits, the standard of data representation in quantum computing, like the bit in traditional computing. The most powerful quantum computer today, the IBM Eagle only has 127 qubits (Sparkes, 2021). While this is an impressive accomplishment nonetheless, the disparity between the current and the theoretical implies that quantum computing is still in its infancy and much more needs to be done before it can reach its potential. However, the largest quantum computer in 2019 was the Google Bristone with just 72 qubits. The number of qubits in the leading quantum computers essentially doubled over 2 years. This is both good and bad news. The good news is obvious because of the benefits quantum computing touts. The bad news is that advancements with quantum computing would likely make brute-forcing advanced encryption schemes possible and render traditional encryption useless. The country that wins the quantum computing race will likely gain a major boost in global influence and national capability. In the hypothetical situation that a foreign nation develops a quantum computer powerful enough to crack encryption or authentication, U.S. Fortune 500 companies, many of which are cloud providers, would be likely targets. U.S. government assets would also be targets, including military and DoD clouds. These collective clouds likely provide the most valuable data to an adversary and have the most impact to the U.S.. From a cloud perspective, it is vital for the U.S. be the front-runners in quantum technology and also come out with the next-generation of encryption algorithms before quantum computing makes traditional encryption schemes obsolete.

3.2 Internet of things

As the "Internet of Things" (IoT) continues to grow to encompass more devices, the threat towards cloud computing also increases. Only a few decades ago, airman had to physically go on base to access a Non-classified Internet Protocol Router (NIPR) computer. Now, it is possible to use technologies such as Virtual Desktop Infrastructure (VDI) or VMWare to access NIPR workstations from at home. Apps also exist to access their emails from their phone. In 2019, the 445th Airlift Wing at Buckley AFB came up with the "Desktop Anywhere" program, which allows Air Force reservists to run a stand-alone Air Force desktop over their personal computers and phones (Amidon, 2019). More recently, the U.S. Army Futures Command has implemented ways to allow soldiers

to access Secret Internet Protocol Router (SIPR) computers from remote locations (DEVCOM C5ISR Center Public Affairs, 2021). The evolution of IoT introduces more devices to military and government clouds, including personal devices. These IoT devices, if not configured properly with security in mind, can lead to increased attack vectors for adversaries.

3.3 Augmented reality

In the past decade or so, life has slowly trended towards a virtual side, with many people opting to shop online, meet people through dating apps, and even buy cars online instead of going to a dealership. COVID-19 further accelerated this change, making virtual concerts, virtual hangouts, distance learning, and teleworking the norm. Adjacent to this is augmented reality and virtual reality, which include entire industries built on making virtual representations of the real world. Just recently, Facebook publicized the imminent release of the Metaverse, which is a virtual extension of the real world that people can plug into and access (Clark, 2021). Many service members will, no doubt, plug into the Metaverse and its applications will eventually be adopted by the DoD to enhance national objectives. A project of this size will likely be stored in the Cloud. Let's push realism aside for a bit and discuss a hypothetical situation. What if augmented reality allowed soldiers to display a map that showed locations of friendly forces? What happens if the soldier gets plugged out mid-battle? They just lost situational awareness of where their team is. Or what happens if adversaries somehow gained access to the soldier's map? They now know the soldier's location and their entire team's location. The bottom line is augmented reality has the potential to bring in new capabilities for the DoD. However, if augmented reality data is stored in the Cloud, it will be subjected to the same vulnerabilities that anything else in the Cloud faces because the Cloud is a single-point-of-failure.

4. Conclusion

Cloud computing has seen rapid deployment and adoption in the past two decades thanks to its myriad of benefits including minimal user infrastructure needed, amortized spending, elasticity, limitless storage, and more. Cloud computing does not come without concerns, many of which are directly tied to the centralization of data, applications, services, and functionality in one place, which is a key essence of the Cloud. Despite these concerns, the DoD and other U.S. government entities such as the Intelligence Community has embraced cloud computing as means of accomplishing and enhancing national objectives. Many cyber concerns with cloud computing such as concerns with privacy and confidentiality of data, availability of data and services, insider threats, and vendor lock-in have magnified effects and consequences for the U.S. government due to the responsibilities that the government has in relation to national functions and the often-sensitive nature of the data dealt with by government entities. To mitigate some of these issues, the DoD and U.S. government is moving towards leveraging multiple providers to provide redundancy and added benefits. However, the emergence of newer technologies such as quantum computing, IoT, autonomous vehicles, and augmented reality, may lead to more cyber concerns in the future.

References

Almorsy, M., Grundy, J. and Müller, I., 2016. An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

Amidon, E. (2019) 'Desktop Anywhere: Innovation in action' [online]. Available at: https://www.445aw.afrc.af.mil/News/Article-Display/Article/1866787/desktop-anywhere-innovation-in-action/.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., 2010. A view of cloud computing. *Communications of the ACM*, *53*(4), pp.50-58.

AWS Public Sector Blog Team (2017) 'Announcing the New AWS Secret Region' [online]. Available at: https://aws.amazon.com/blogs/publicsector/announcing-the-new-aws-secret-region/.

AWS (2021) 'Amazon S3 FAQs' [online]. Available at: https://aws.amazon.com/s3/faqs/.

Baumhof, A. (2019) 'Breaking RSA Encryption – an Update on the State-of-the-Art' [online]. Available at: https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art/.

Bishe, A. (2018) 'How to optimize cost savings in AWS Marketplace' [online]. Available at: https://aws.amazon.com/blogs/awsmarketplace/how-to-optimize-cost-savings-in-aws-marketplace/.

Chen, Y., Paxson, V. and Katz, R.H., 2010. What's new about cloud computing security. *University of California, Berkeley Report No. UCB/EECS-2010-5 January*, *20*(2010), pp.2010-5.

Clark, P. (2021) 'The Metaverse Has Already Arrived. Here's What That Actually Means' [online]. Available at: https://time.com/6116826/what-is-the-metaverse/.

Department of Defense (2018) 'DoD Cloud Strategy' [online]. Επιμέλεια D. of Defense. Available at: https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF.

Department of Defense (2021) 'Future of the Joint Enterprise Defense Infrastructure Cloud Contract' [online]. Available at: https://www.defense.gov/News/Releases/release/article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/.

DEVCOM C5ISR Center Public Affairs (2021) 'Army Futures Command enables classified work from remote locations' [online]. Available at: https://www.army.mil/article/244545/army_futures_command_enables_classified_work_from_remote_locations.

Ďulík, M. and Junior, M.Ď., 2016. Security in military cloud computing applications.

Earnest, L. (2016) 'Who invented Timesharing?' [online]. Available at: https://web.stanford.edu/~learnest/nets/timesharing.htm#:~:text=The%20first%20commercial%20timesharing%20system,and%20began%20working%20in%201965.

Office of the Inspector General (2016) 'DoD's Efforts to Consolidate Data Centers Need Improvement' [online]. Available at: https://media.defense.gov/2016/Mar/29/2001714226/-1/-1/1/DODIG-2016-068.pdf.

Google (2021) 'Discover our data center locations' [online]. Available at: https://www.google.com/about/datacenters/locations/.

Hayes, B., 2008. Cloud computing. Vol. 51 No. 7, Pages 9-11.

Kay, G. (2022) 'A 19-year-old security researcher describes how he remotely hacked into over 25 Teslas' [online].

Khalil, I.M., Khreishah, A. and Azeem, M., 2014. Cloud computing security: A survey. *Computers*, *3*(1), pp.1-35.

Miller, J. (2021) 'As C2E gets going, DIA sets its strategy for more cloud services' [online]. Available at: https://federalnewsnetwork.com/ask-the-cio/2021/04/as-c2e-gets-going-dia-sets-its-strategy-for-more-cloud-services/.

Moss, S. (2020) 'CIA awards multibillion C2E cloud contract to AWS, Microsoft, Google, Oracle, and IBM' [online]. Available at: https://www.datacenterdynamics.com/en/news/cia-awards-multibillion-c2e-cloud-contract-aws-microsoft-google-oracle-and-ibm/.

Platform One (2021) 'WHAT CAN PLATFORM ONE DO FOR YOU?' [online] Available at: https://p1.dso.mil/#/.

Serbu, J. (2016) 'IBM wins $62 million contract to run private cloud pilot at Army's Redstone Arsenal' [online]. Available at: https://federalnewsnetwork.com/army/2016/10/ibm-wins-62-million-contract-run-private-cloud-pilot-armys-redstone-arsenal/.

Seredynski, P. (2021) 'Gathering clouds will form autonomy's computing backbone' [online]. Available at: https://www.sae.org/news/2021/04/autonomous-vehicles-and-their-cloud-computing-networks.

Sparkes, M. (2021) 'IBM creates largest ever superconducting quantum computer' [online]. Available at: https://www.newscientist.com/article/2297583-ibm-creates-largest-ever-superconducting-quantum-computer/.

Srivastava, P. and Khan, R., 2018. A review paper on cloud computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(6), pp.17-20.

Statista Research Department (2014) 'Number of consumer cloud-based service users worldwide in 2013 and 2018(in billions)' [online]. Available at: https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/.

Szmigiera, M. (2021) 'Leading countries by gross research and development (R&D) expenditure worldwide in 2021' [online]. Available at: https://www.statista.com/statistics/732247/worldwide-research-and-development-gross-expenditure-top-countries/.

Office of the Federal Chief Information Officer (2021) 'Data Center Optimization Initiative' [online]. Available at: https://datacenters.cio.gov/.

Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), pp.583-592.