A Study of Security and Privacy Issues and Disagreements Concerning Cloud Adoption and Efficient Use

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Andrei Stan

Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature ____ Date __________

Andrei Stan

Approved ____ Date __________

Sharon Tsai-hsuan Ku , Department of Engineering and Society

Introduction

Cloud computing offers many benefits over traditional workloads. However, security in the cloud, in many cases, is very different to how it is handled traditionally. User data and processing is done in data centers owned by service providers like Amazon Web Services(AWS) and Microsoft, which presents logistical issues like physical data center security and access as well as sociotechnical issues like the proper use of customer data and its ownership.

It is important to contextually define security and privacy in a cloud computing environment to describe the need to protect data of all kinds from unintended access as well as protecting and maintaining more qualitative measures regarding the level of confidence in the ability of both sides of a cloud service agreement (user and provider) that the other party will follow the guidelines set across to ensure intended access and use.

Security needs always exist, but particularly in the public sector, intelligence agencies or government contractors need an assurance of the same level of high security that they are able to achieve with their on-site infrastructure. In order to match this, service providers may have accreditations or certifications that, at a technical level, show qualification to handle potentially confidential or highly classified workloads. This means being able to handle the data in such a way that it is not accessed by unintended parties such as those not holding a sufficient level of clearance or those that are simply trying to access it from outside to use for purposes other than government business. This is true of any sector of business using some form of restricted data, public or private. In any case that there is a breach or inherent insecurity, the trust that the company has in the cloud service provider diminishes very quickly, leading to an underuse of an otherwise extremely capable technology that adds another dimension to traditional computing.

Even when the technical qualifications are met, social disagreements may occur. Individuals on both sides may have negative predispositions which cause them to be particularly skeptical or concerned about the safety and privacy of their data. Assurances like highly restricted physical access to data centers may even serve to deter certain users, especially those with prior distrust towards service providers or the industry as a whole.

Documentation from service providers and accreditors can be used to understand the technical aspects of different levels of workload security. This documentation can then be compared with records of high profile failures in order to potentially identify core issues that lead to some of the problems with security and privacy in cloud computing.

Literature Review

Cloud benefits and tech aspects were found to be the most important when considering cloud adoption(Khayer et al., 2020) but resistance to change and computer self-efficacy are also important. This is expanded by describing a divide between, at least in Europe, areas of differing economic and technological development in terms of factors that influence cloud adoption. Arvanitis, Kyriakou, & Loukis (2017) found the less developed Southern Europe to be concerned with financial issues while the more developed Northern Europe to be more concerned with factors involving business efficiency, like increased innovation and capabilities.

Security was found to be an issue for cloud adoption for students in educational environments as well (Arpaci et al., 2015). It was also found that perceived security is the deciding factor when considering cloud adoption and use. This can be influenced by assurances but initial perception was found to have a bigger effect. This is consistent with the findings of Shah et al. (2014) in that website design had the biggest effect on perceived security as opposed to what would be expected to have a larger impact in terms of assurances (both external and internal) and the solutions actually available for confidentiality.

This social perception was also found to be mainly affected by education about cloud terminology and concepts, at least in the Jordanian government context. Different countries will behave differently but a lack of education in this context led to some subjects confusing terms as well as having opinions that did not match real world facts (Alkhwaldi, Kamala, & Qahwaji, 2019).

These concerns do seem to have basis however, according to King & Raja (2019), who highlighted the need for regulatory reform as far as the foundations of security and protection of sensitive data in cloud computing. They argue that current definitions of sensitive data are not adequate for proper protection of users or for the success of cloud service providers. Contrasting these perceptions, however, cloud adoption has several methods for handling security and privacy issues. These methods are well documented in the context of AWS and Azure (Rath et al., 2019) as well as many other providers. The benefits of cloud are also well known but the issues seem to center around security once again, at least in the context of e-government (Alshomrani & Qamar, 2013).

On the opposite side, Hughes et al. (2019) propose a new idea of not segregating cloud service use by governments. They suggest the lack of potential for things like GovCloud in terms of growth and propose the use of the public, widely available, and continuously growing cloud using special security techniques in order to place the responsibility back in the hands of customers with respect to government or classified workloads.

The trend around cloud adoption issues seems to be focused around security and privacy, specifically in terms of perceptions and individual opinions. There seems to be some disagreement, especially because of lack of education about cloud concepts and security practices. The arguments that there is a lack of a proper definition of cloud security line up with this, hinting that there may be more than just a lack of education or widespread knowledge but more so an inherent disagreement about what security in the cloud is or should be. There may be more to this than just the idea that users are quick to conclusions based on first impressions but rather that, the amount of mismatch between their expectations and actual cloud security practices is enough to set off an alarm and cause inherent concern.

STS Framework and Research Methods

The issues regarding sensitive cloud data can be labeled as ones of society as well as technical. The frameworks chosen for analysis of these issues are relevant to this type of classification and attempt to understand these issues. Hughes' perspective was used in order to understand the sociotechnical aspect behind the information. A SCOT analysis was used to target the specific social groups at play as well as their interests and conflicts. Finally, ANT analysis was used to combine the issues and identify the actants at play as well as their translation as part of the identified ANT network.

Hughes' Perspective Analysis:

The builders behind cloud storage are mainly the developers and engineers behind the specific services. They obviously work on the programming, hosting, and software-level security of the systems. Additionally, there are support teams and maintenance personnel that are responsible for running these services and catering to customers. Pertinent specifically to the topic, the maintenance personnel are often a majority of the few people that have access to the physical data centers that house the cloud storage. In addition to maintenance staff, third party auditors also play a role as “system builders” by providing a security safety net and potentially reassurance of the security of the services to customers.

In the case of AWS, the most important voice is the customer, per their “working backwards” process. Customer demands are said to be directly implemented in the majority of cases. Politically, there are also many customers in the public sector that have a big stake in how these services are developed and maintained. Increased security is required for customers in the intelligence and defense communities. These customers can be seen as major stakeholders, especially in cases like the dispute over the $10B Pentagon JEDI contract between AWS and Microsoft.

There are also differences that cause customer preference between providers. In AWS’s case, being the biggest provider, their main selling point is the high availability offered by their infrastructure. In Microsoft/Azure’s case, the main selling point is that they are able to offer their services at a much cheaper price due to hybridization integrated into the native Windows environment. Smaller cloud providers also specialize in certain services, with the example of Oracle being one of the most experienced database service providers or IBM having spent the majority of their resources recently specializing in artificial intelligence and machine learning services.

With cloud computing being at the forefront of current computing technology, there are not very many reverse salient aspects that are due to age. Many can be identified as “growing pains” like the slow adoption of the services themselves by customers due to a large gap in expertise between providers and customers. Once again though, the security of the cloud is a huge issue. The fundamental idea of storing private data or records on external hardware, potentially accessible by other people outside of a specified group is something that cloud computing has no clean solution for. While governance, policies, and certifications attempt to ease some of these concerns, there can never be any assurance other than trust and laws or regulations that can completely remove these concerns.

The public sector adaptation of this technology is the biggest driving factor in the adoption of cloud services. Security is a concern but the example of intelligence agencies and defense organizations adopting these services for mission critical and highly secure workloads serves as good motive for other, private sector or individual customers to put their trust in the security behind cloud services.

It is, however, very difficult for this to happen. The transition of government infrastructure, which in large part is a completely separate technological entity to the rest of the technological world, requires highly skilled and specialized designers and builders to aid in a transition to cloud computing. It is not as simple as the rest of the computing needs of the private sector in just a transition over the internet. Builders that specialize in these specific technologies, who until recently have been largely working internally at many of the government services in question and are now working with cloud providers, must use their knowledge to adapt these highly specialized systems to cloud usage. Even something as simple as data migration cannot be handled through a simple internet transfer and new methods, like physically secure storage media transported through physical means like armored vehicles, must be employed to allow this kind of adoption.

SCOT Analysis :

In the context of cloud storage security, there are only a few relevant social groups. Users make up the entirety, with the different types having different needs or regulations governing their decisions. In the private sector, users range from single users like students to multi billion dollar, Fortune 500 corporations like Capital One, General Electric etc. In the public sector, users include contracting firms, universities, and even defense organizations like the FBI and CIA.

Cloud security considerations vary among these different types of users, ranging from little to no consideration for smaller customers in the private sector like students to a top priority, such as for defense agencies. These users that require a high level of security even go as far as operating completely disconnected from the internet, through SIPRnet and JWICS. For customers that operate on the internet, namely users in the private sector, security considerations also widely vary, especially in the case of intellectual property being stored in cloud services by larger companies and even by some individual users.

These requirements can sometimes be negotiated. Especially in the private sector, some users are willing to compromise on security in order to use cloud services. This is not, however, common. Most users that do have security requirements are not at all willing to budge, and cloud service providers often know this. Most services are built around the idea that security is the highest priority. This can especially be seen in the implementation of public sector cloud technologies, with many data centers being explicitly dedicated to certain customers and solutions like dedicated servers/storage being offered to allow for stricter control of data access. Closure mechanisms do exist but the fact still stands that the services that cloud providers offer run through non-privately owned hardware. A physical person or group of people not employed by the customer has to have access to the physical hardware in order to guarantee that the services continue to run. Third party auditors exist to give the customers a sense of relief in that the physical hardware and data centers are inspected and certified to meet certain security standards and compliances like FedRAMP, ITAR, FERPA etc. There are also those data centers in which, if required by the users' workloads, all personnel are required to meet certain clearances, such as secret or top secret, in order to even be allowed to access the data centers.

This adds additional complexity to the interaction between provider and user. There is the human element involved in all of these interactions, which is always the quickest to give way to breaches. Systems may be secure, networks may be restricted, data centers may be locked down, but the human aspect, whether it be a careless data center employee leaving a door open, an auditor that simply signs off on inspections without actually checking the systems etc. will always sit on the back of the minds of users that have the highest security requirements.

Providers are aware of this and work to try to mitigate these factors. This interaction between humans, regardless of the security properties of the systems, remains the bottleneck for adoption and leads to a question of how the interactions between provider, user, and third-party auditors can be altered or improved to help move past what is possibly the biggest barrier to entry for cloud computing in interpersonal trust.

ANT Analysis:

A human-non human network is identified to address the concept of limited physical data center access as well as societal perception of cloud adoption. This network centers around the idea of careful control of processing and data specific to workloads with highly sensitive data directly conflicting with the policies in place at most cloud providers that are created for the very purpose of high security. While on one side, the idea of limiting physical data center seems like the perpetrator in that it may cause a lack of trust, the societal aspect serves as an issue in this network as well as it may have a non-pragmatic view or perception of cloud and of what actually happens "behind the scenes" in said data centers.

There is some successful translation here because the concept of a black box of computers that handle workloads in highly classified environments directly contrasts the idea of careful handling by humans of the data. When an issue arises over this generalization of data centers and data handling, the societal aspect of the human stakeholders and decision-makers in cloud adoption can now be seen as that of an obstacle in the way of adoption and further development. The actual policies and handling of the data center access policies can be seen as a malicious tactic to either steal customer data or sell it for profit. It is likely only in these situations, when circumstances like negative predisposition towards cloud adoption or malicious intent on the side of the physical data or processing side is present, that this translation can come across.

The concepts can be somewhat explained by the actant network. They are symbiotic characteristics where the societal view and general uneasiness about privacy comes as a result of previous issues and failures that have caused people to be more aware and place a greater value or importance on their sensitive data. This very same uneasiness has led to the development of such strict measures as the level of control of the physical data centers or the encryption and control of such things as access keys. These measures, while intentions may be good behind their establishment, can directly contrast societal opinions and create a positive feedback loop of distrust and stricter control further driving apart the middle ground solution for the proper sensitive data handling procedures.

The lack of proper cloud education and the extreme specialization of the field also causes issues as far as societal opinion. Even though certain providers continue to improve their standards for ensuring security implementation ease-of-use, breaches continue to happen, with an ever-increasing magnitude of implications. Opinions are developed (whether based in fact or not) by all who become aware of the issues, which serve to further drive the idea that cloud providers have little interest in protecting user data. Further combining this with the feedback loop of increasing security to counter breaches leads the public opinion further towards the idea that there is something to hide, and that trust can never be placed completely in providers' hands.

Further looking into societal opinion, the SolarWinds breach and its implications as far as updates to a system (Massacci et. al., 2021) is a good example of the types of mistakes made by providers in terms of security. Central to security in computing has always been that the newest update or patch is inherently the most secure. Massacci et. al describe the implications of this, with many providers not even allowing users to avoid most updates. This obviously leads to situations where, when an update like the one that led to the SUNBURST vulnerability is released and forced upon users, societal perception goes even further towards the opinion that providers are uninterested in security or that their only concern is in profits.

While it is not false that provides' main scope is that of profits (as business entities which mostly exist in an incentive-driven mixed-market economy), the profits themselves rest in user trust and confidence that the systems they are purchasing, especially with the large costs that cloud scale often implies, will protect their data at the same level or even better than what they are able to provide by themselves. Businesses are aware of this because they have to be, with updates being created in some part to add new features, but with the main purpose of improving systems and keeping the target constantly moving for attackers. It is naive to say that "breaches will happen, that's just IT" but the point still stands that even when a breach does happen, it does not mean solely that providers are careless or not user-focused. Societal opinion that heavily tends towards a focus on failure and not on the response to those failures combined with the ever-increasing change to policy that may create frustrating circumstances for users drives the conflict between the user and provider further and creates deeper and deeper distrust.

Mediation considerations:

Using the concept of data sovereignty can help with understanding the complex relationship of data privacy between users and providers in the cloud. Within the shared responsibility model, the user does have control over encryption and secure communications to ensure that data privacy is protected both in transit and at rest. In order to accomplish this, however, the user must use the CSP(Cloud Service Provider)'s services.

The transit of the data or the storage must still be done by the CSP. At rest, the user must rely on the CSP's hardware. In transit, they must rely on either the network, the infrastructure, or, in some cases, the vehicles and hardware that the CSP uses to migrate data. The question arises of whether or not then the user even has full control over their data. Yes, they are the only ones that have access to it since encryption makes it so they are the only ones that can make sense of the data. In this case, however, it is still reliant on the CSP's hardware to enable the encryption and storage. Yes, the users are the ones who, at the end of the day, have the final word on what happens to their data. However, if they say they want their data back and out of the CSP's hands, there is often a payment associated with data export. CSPs also give the guarantee that they do not touch the data that the user keeps on their services but, because of security restrictions with the physical data centers that house data, the user also does not have this privilege of "touching" the data.

This specific scenario unintentionally creates a mediation of the "touching" of data. The concept of touching the data, since neither CSP nor users have access to the physical hardware (both in different contexts but netting the same result), is now one of imagination. The technology of the cloud makes this a trust issue, and thus a social issue. The encryption of the data, the deletion and destruction of material but also the privacy and security are now all up to trust in what the system says. In the example of encrypted data, the CSP must treat the data as a sensitive virtual package, with no knowledge of what is inside or what it is being used for (whether good or bad purposes). There is no guarantee however, that this is fact since, by their own terms and services, they are not allowed to double-check.

On the user side, there must be trust in the CSP such that saying that data is being exported, encrypted, or deleted is actually what is happening. The user is only capable of seeing what the CSP provides and has nothing other than a guarantee that what they are told and shown is in fact the truth, with no way to double check it because of the inherent physical access restrictions.

Trust then is the only mediator that can make this system functional. With no way to guarantee proper behavior for either side, the trust and understanding between the human elements of both the user and CSP absolutely must be present to allow the system as a whole to work.

The question still remains, however, of who owns the data when the system does work. Assuming trust is in place and that both parties adhere to their agreements, the CSP does not have access to the data but, other than through the CSP's services, neither does the user.

It is tempting to say that the user is the owner and is simply using the services of the CSP to house it, almost like using a storage unit or keeping one's belongings in a rented home. In many cases however, it is not as simple as the user just storing their data on the cloud. There are many cases when the user even uses cloud services to create the data. When this is the case, and the CSP is responsible for everything about the data from creation through storage the user's only responsibility is telling the system what to do. Even this is sometimes not the case however since there are many instances, especially for bigger, newer users, when employees of the CSP help the users set up their infrastructure to the point where the only action taken by the user is to give the ‘green light’ for whatever it is that they want done.

In this case, the user becomes somewhat of a landlord for their data, technically owning it but with the data only having any value while the CSP is providing services for it. The CSP also needs the consumer to remain satisfied and pays something like trust rent in order to ensure this. Without this trust rent, the user has no choice but to lose confidence and switch to a different CSP as the new renter of their data. Policies like the export cost for data can be effective for smaller, less financially capable users, but ultimately serve only as a minor annoyance for customers whose primary concern is transparency, trust, and a privacy guarantee from the CSP.

Data Analysis and Discussion

Issues around cloud security seem to be focused mainly on perception of security and privacy, in terms of education about formal definitions or applications or predispositions due to world events. Transition to cloud however is here and these issues create problems when it comes to adoption.

The findings of Norris & Reddick (2012) show that the transition to cloud may not be at a point of revolution and likely never will be. They found the transition of governments to electronic domains to be more of an incremental shift rather than a revolutionary one in the context of local e-governments. This can be interpreted as either agreeing or disagreeing with the findings of Hughes et al. (2019). Both a transition to segregated government sub-clouds and the idea of using public cloud in specialized manners but en masse can be considered examples of revolutionary changes and both can also be considered incremental as both are examples of using what is already available and slowly and effectively leveraging current resources for government purposes. This would depend on the context of the use and again, is very specific to each user’s perceptions, needs, and capabilities.

An example of the current lack of education can be identified from the Capital One breach on AWS a few years back. AWS splits security responsibilities between the user and provider in that they handle “security of the cloud” (infrastructure, physical security, measures and encryption options) while the consumer handles “security in the cloud” (end to end encryption, data access permissions etc.). Because of this as well as some design choices concerning the immediate display of information in the AWS console, specifically, large-scale creation of S3 storage buckets, Capital One reached a point where one of their critical S3 buckets was left public and breached by attackers. This led to data being “decrypted and exfiltrated from the account” (Corstorphine, 2020).

This leads to a discussion of blame, and who takes responsibility for incidents when breaches or other unintended events occur. AWS calls the previously mentioned split the Shared Responsibility Model. The initial impression may be that AWS is simply trying to put the responsibility and thus the blame for any incident that falls on the “security in the cloud” category into the user’s hands. However, the implications of this are much deeper. AWS guarantees handling of the issues that users would typically have to worry about in their “security of the cloud,” not pawning off the rest on the user but rather allowing precise control to and a level of confidence that their data is controlled in exactly the way that they intend. This is even as far as allowing the user to encrypt data in such a way that AWS would not be able to access the data in a meaningful way, almost like guarding someone else’s bag without having any idea or any way to understand what is inside. This targets the issues around the discomfort that users feel when considering that their private, highly sensitive data is being put in another party's hands with nothing more than a written guarantee of security in return.

This is especially an issue in the public sector and for security agencies. Private sector companies are typically more open to the transition since their data simply requires some level of security in order to ensure either end user privacy or simply, to protect trade secrets or information. Breaches in either of these categories of data ultimately only lead to business consequences, revolving around reputation and loss of revenue or exclusivity, and affecting mainly the reputation of leadership and security professionals in that business entity. Hackers or malicious users in these circumstances are typically small groups or single individuals with motivations mainly around monetary gain (through selling or use of accessed data) or social impact (whether through commentary, raising awareness for their own opinions, or simply as a test of abilities).

On the other hand, the same type of breach on the public sector side could lead to much more severe consequences, potentially having international effects. A breach of security of sensitive data would not just be things like user profiles on an app or contact information, banking details etc. but could go as far as putting social security numbers, criminal history, or other highly confidential information for not just users but for the whole population at risk of exposure. It may even lead to unintended access of highly secretive government information about other countries which could lead to an unending list of severe consequences that impact the country or world as a whole.

For these reasons, many entities in the public sector that use cloud services host their information on a completely separate portion of the particular provider's infrastructure. In AWS's case, any government communication that requires a level of clearance goes through two completely separate cloud environments, the Secret and Top Secret regions. Not only are these regions only accessible by SIPRNet (Secret Internet Protocol Router Network) and JWICS (Joint Worldwide Intelligence Communications System) respectively, rather than the worldwide internet, but the AWS employees that handle interactions with these types of users are required to hold the respective clearance and handle communications through secure, limited access physical environments called SCIFs (Sensitive compartmented information facility). They are actual physically enclosed rooms that all communication concerning certain topics is required to go through. This goes the majority of the way in preventing hackers that may be as large as entire national entities, attempting to access information that could have, as mentioned above, global effects when in different hands.

It is also important to understand the priorities of both sides in terms of security and privacy. The "security" of a cloud implementation has many aspects, some unique and some inherited and even amplified from traditional computing, additionally even further split among users and providers (Mthunzi et al., 2019). Public cloud implementations specifically put a target on a cloud system through simple presence on the system as well as add additional areas of exposure through malicious insiders or elevated risk of DDoS attacks. Users tend to focus more on these issues, summarized as a feeling of loss of control. Providers' view is more centered on governance of data security in terms of maximizing control while maintaining reasonable access. There is a big difference in priorities here. Overlap is in areas to be expected like availability, resiliency, reliability, and durability. However, there is enough of a separation of priorities to be able to say that the definition of security for both sides is different.

Cloud computing is a constantly evolving field and this disagreement in priorities is to be expected since the security landscape changes with it. The issues of solving the Capital One

Breach is simple: avoid future miscommunication and improve the user interface. This does not, however, automatically guarantee the prevention of future issues. The social aspect of the disparity in security definitions, and therefore needs and priorities, must be addressed first before any technical changes are made.

Both sides have a need for each other. The constantly evolving technological needs of public agencies fit well into the capabilities of cloud systems and cloud service providers' ideal customer is one like public agencies, with a large, constantly growing, persistent need for their services. However, a simple written guarantee will not persuade skeptical users and a provider will not be persuaded to change their healthy systems for a single customer. Their priorities and interests must be taken into account so that relevant changes can be made to the policies and expectations of both sides.

Conclusion

The problem of adoption and trust in cloud computing can be initially interpreted as one of lack of development, education, and communication. However, even once simple solutions have been put in place to fix all those issues, the sociotechnical issues boiling down to definitions, understanding, and expectations of security and privacy still stand in place of smooth cloud adoption. The strengths of cloud computing become its biggest weaknesses in that the rapid expansion and development that make it so useful and reliable for use by customers with all types of workloads, from small, private sector businesses, to the largest multinational, Fortune 500 corporations, to highly secretive intelligence agencies, are also its downfall. The same rapid expansion and development make defining and enforcing security and privacy effectively near impossible at a consistent, easy to understand level. More care has to be taken not just in ensuring security and privacy but rather making sure the understanding and definition of those concepts is unanimous among providers and customers to be able to provide guarantees and expectations that leave very little room for surprises on both sides. Focus has to be shifted towards educating on concepts, definitions, and human interactions in addition to technical aspects. Future work should focus on finding ways to incorporate this into cloud adoption in a way that it becomes natural and expected.

Bibliography

Alkhwaldi, A., Kamala, D. and Qahwaji, P., 2019. Security Perceptions In Cloud-Based E-Government Services.

Alshomrani, S. and Qamar, S., 2013. Cloud Based E-Government: Benefits And Challenges. [online] Ijmse.org. Available at: <http://www.ijmse.org/Volume4/Issue6/paper4.pdf>.

Arpaci, I., Kilicer, K. and Bardakci, S., 2015. Effects of security and privacy concerns on educational use of cloud services. Computers in Human Behavior, 45, pp.93-98.

Arvanitis, S., Kyriakou, N. and Loukis, E., 2017. Why do firms adopt cloud computing? A comparative analysis based on South and North Europe firm data. Telematics and Informatics, 34(7), pp.1322-1332.

Corstorphine, A. (2020). The Capital One Data Breach a Year Later: A Look at What Went Wrong and Practical Guidance to Avoid a Breach of Your Own - Security Boulevard. Retrieved 14 February 2021

Hughes, J., Munson, C., Schear, N., Patel, R. and Kalke, M., 2019. Classified As A Service (ClaaS). [online] Apps.dtic.mil. Available at: <https://apps.dtic.mil/sti/pdfs/AD1100938.pdf>.

Khayer, A., Talukder, M., Bao, Y. and Hossain, M., 2020. Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach. Technology in Society, 60, p.101225.`

King, N. and Raja, V., 2012. Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), pp.308-319.

F. Massacci, T. Jaeger and S. Peisert, "SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing With the Devil?" in *IEEE Security & Privacy*, vol. 19, no. 02, pp. 14-19, 2021. doi: 10.1109/MSEC.2021.3050433

Mthunzi, S. N., Benkhelifa, E., Bosakowski, T., Guegan, C. G., & Barhamgi, M. (2020). Cloud computing security taxonomy: From an atomistic to a holistic view. Future Generation Computer Systems, 107, 620–644. https://doi.org/10.1016/j.future.2019.11.013

Norris, D. and Reddick, C., 2012. Local E-Government in the United States: Transformation or Incremental Change?. Public Administration Review, 73(1), pp.165-175.

Rath, A., Spasic, B., Boucart, N. and Thiran, P., 2019. Security Pattern for Cloud SaaS: From System and Data Security to Privacy Case Study in AWS and Azure. Computers, 8(2), p.34.

Shah, M., Peikari, H. and Yasin, N., 2014. The determinants of individuals' perceived e-security: Evidence from Malaysia. International Journal of Information Management, 34(1), pp.48-57.