Please cite as: Kevin Curran, Eugene McNamee, Niall McCaroll, Priyanka Chaurasia, Shaun McBrearty (2019) *The Security Considerations in Cloud Adoption for Legal Firms.* ICSET 2019 – International Conference on Science, Engineering & Technology, Tel Aviv, Israel, 29-30th March 2019

The Security Considerations in Cloud Adoption for Legal Firms

Kevin Curran[1], Eugene McNamee[2], Niall McCaroll[1], Priyanka Chaurasia[1], Shaun McBrearty[1]

[1]Ulster University, School of Computing, Engineering and Intelligent Systems, Londonderry, Northern Ireland

[2] Ulster University, School of Law, Jordanstown, Newtownabbey, Northern Ireland

Abstract - Cloud computing delivers various benefits to legal departments, law firms, and professional services firms, particularly those operating globally. Driven by the need of greater client expectations and access to data remotely, law firms have started to adopt cloud computing. A low-cost alternative, flexible, and on-demand services are the key features of cloud computing. However, the extent to which law firms should use cloud services is still bleak. Cloud systems, like all IT developments, possesses a new set of risks. The digital transformation of the legal sector raises concerns about how to handle sensitive client data without compromising confidentiality. In this paper, we summarise factors that drive the adoption of cloud by law firms, issues faced in handling sensitive data, challenges in cloud adoption, and emerging techniques for secured cloud storage.

Index Terms— Cloud Computing, Legal Technology, Cloud Security, Legal computing

I. INTRODUCTION

Law firms are faced with a choice between security and usability when sharing confidential documents with authorised third party and clients. Sensitive information such as customer details, case documents, tax and financial records or intellectual property could be leaked causing severe reputational damage to a law firm [1, 2, 3]. Consumer file-sharing services have become popular such as Dropbox and Google Drive, however, security protections are weak and therefore the confidentiality of documents can be exposed when using such services. The US National Institute of Science and Technology (NIST), defines Cloud computing as "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [27].

More and more services and accompanying data are being moved to the cloud. There are several advantages to using the cloud over on-premise. For instance, the cloud offers flexibility in that a company can offer a service prior to purchasing all the hardware needed as in the pre-cloud days. The real power of using the cloud is that it can instantly meet the demand due to the large capacity of the provider's remote servers. This will continue to allow companies to estimate costs more predictably (especially start-ups) as they can incrementally add on services when needed and resources allow. It will also lead to a lower carbon footprint for organisations as a result. No over provisioning anymore. Therefore, in the short-term, companies will buy less dedicated hardware in the form of servers and move to renting capacity as needed in the cloud [21, 22].

The cloud is also enabling organisations to move away from the traditional "perpetual license" and adopt annual licenses. Cloud customers also like the lower costs of a monthly subscription as opposed to an upfront larger perpetual license fee. The main reason of course that companies are moving to the cloud is the ability to eradicate software piracy through online authorisation. There are savings to be made for the consumer too due to the cloud license model as controlling licenses from the cloud eradicates the responsibility of ensuring that every copy of installed software has an authentic up-to-date license.

A Spiceworks Market Insights survey found that out of 500 IT professionals from small and middle size organisation, half of the employees were already using consumer cloud-based file-sharing services on their own but in many cases, this was out of the control of the IT policies of their organisations [1]. However, there are more secure consumer file-sharing solutions referred to as business or enterprise solutions. There are many benefits to using cloud computing not least cost effectiveness and increased productivity. The mobility of the workforce can also be increased by going virtual and removing the requirement to be physically located at the office. A range of technology exists to enable virtual practice such as file-sharing and audio/video (e.g. Skype, GlobalMeet, or GotoMeeting) that can be used to manage file online and communicate with clients. There are also a variety of specific legal online management systems that enable virtualisation. Cloud computing is increasingly omnipresent, even in law firms, despite the view that the legal profession has a reputation for being slow to adapt to new technologies. It is particularly popular among small firms and sole practitioners [20]. If a data breach occurs, and the associated data is retrieved in plaintext form, an organisations worst nightmare has become a reality [25]. What follows is typically a slew of press releases, negative publicity, damaged business reputations, and fines under various data protection laws. To reduce the impact of potential data breaches (and to provide privacy for CSP consumer data) CSPs typically employ the use of cryptography. We look here at the trend towards cloud adoption by legal firms and the role of data security in securing legal documents in the cloud.

II. DRIVERS OF CLOUD ADOPTION

The capacity in which the cloud computing is being used by law firms depend on the size and nature of the firm. A study conducted by International Legal Technology Association in 2013 listed five key use of cloud computing in law firms as: backup (55%), recovery (50%), email (35%), document management (29%), and case management (18%) [4]. Other cloud services that have become popular are data centres, spam filtering, and mobile data management [4]. Firms rely on cloud-based services such as electronic discovery for legal proceedings and virtual data rooms for transactions. Besides, the structural transformation in addition to outsourcing, increasing client expectation, mobile adoption, and boom of Big Data have driven the cloud computing advancement.

Disaggregation of large firms: Firms are commonly restructuring triggered in part by corporate client's reluctance to pay extensive legal fees and overhead. As a cost reduction, firms have started to replace fulltime services with flexible and on-demand services. Recently, cloud-based systems have been increasingly used by large firms to provide services across different locations. There is a pressure on lawyers to cut down the operational cost which has let to growth of virtual law firms. These law firms have network of lawyers at different locations, including some at client sites who operate using cloud-based systems [5].

Growing client expectations and lean business model: Clients have become accustomed to do much of their businesses online, and hence expect law firms to provide their services online [4]. With iterative expansion of products and services, lean business models have become popular in legal occupations. Consequently, law firms are more inclined to add staff and services on-demand instead of large upfront capital investments. This scalability of lean business model aligns with the metered services provided by cloud computing leading to increased cloud adoption [6].

Big Data and mobile: Two important technology trends, Big Data and mobile have also encouraged adoption of cloud technology by law firms. 91% of lawyers now use smartphones and 48% use tablets [5]. Addition of mobile devices have increased efficiency and the use of cloud computing serves a key role in accessing and syncing files between multiple cloud platforms. Similarly, cloud computing is used to store Big Data collected by large firms [5]. Within small and medium size law firms, the adoption of cloud becomes more challenging. The key obstacle for small and medium sized enterprises (SMEs) in cloud adoption is how the software and hardware match and interoperate with each other when executing core business applications [12]. Therefore, SMEs willing to migrate to cloud need to know how to handle this issue as the market is dominated by big cloud service providers (CSPs). In [12], a general framework for cloud adoption is proposed for SMEs (Figure 1).

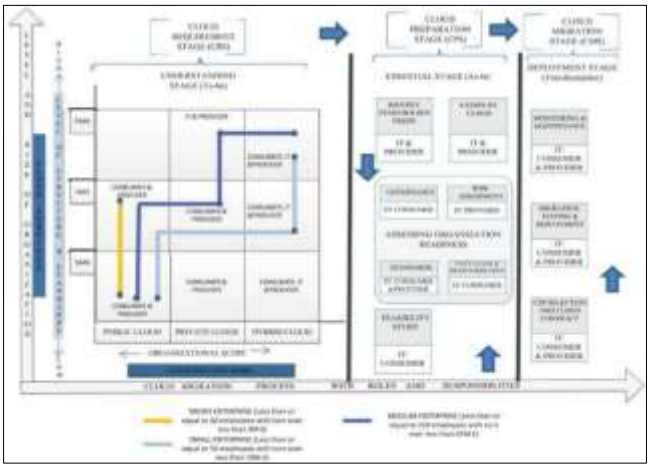

Figure 1: Framework for cloud adoption by SMEs [12].

The framework comprises of three stage migration process: preparation, requirement, and migration. In the preparation stage, the type of computing services and deployments suitable for SMEs is assessed based on size, nature of business, and turnover. The requirement stage allows the enterprise to do a feasibility study, assess organisation readiness with respect to governance and risk, and identify stake holder needs. In the migration stage, the CSP is finalised and the contract is signed, followed by testing, deployment, monitoring, and maintenance [12].

Organisations should also be aware of that smaller cloud providers could close. It happened to a provider called 2e2 (Bell, 2013). E2e asked customers for £1m if they wanted uninterrupted services and access to their datacentre facilities. Of course, most wanted to access their data immediately so that they could migrate the data and applications to another service provider. but the company stated that "this process could take up to 16 weeks and we will need to ensure that the integrity of third-party data and security is maintained". In other cases where cloud providers were going out of business, customers were notified and given adequate time to transfer their data elsewhere. This is less likely of course to occur where larger cloud organisations such Amazon, Google or Microsoft are the provider

III. DATA SECURITY IMPLICATIONS

The cloud can also relieve businesses of the need to implement burdensome disaster recovery plans as cloud providers take responsibility for implementing backups and maintaining a live stable environment. There is also much savings to be made for large businesses when performing maintenance especially with regards updates as the provider can roll these out. This aspect alone make cloud computing an attractive option. It also can be argued that cloud computing environments are more secure as dedicated skilled IT admins deal with security patches & updates. The trend seems to be for increased usage and reliance on cloud services. Ultimately it does make sense. If an organisation of for example, 5000 employees is served by an IT dept of say 10-15 staff (which is not unusual). Then apart from the usual servicing of client machines/desktops etc - they also have to ensure the email server and all relevant internal network

services are secure. All this must be balanced with daily workloads. On the other hand, they can offload email to a large multi-national cloud provider with scores of dedicated workers serving that product. It can be more difficult for an average organisation to have similar trained security personnel. The future seems to be that if a small pool of Cloud Giants servicing a large pool of minions. Collaboration benefits as well as apps and documents can be synchronised seamlessly and updated in real time. The cloud is a natural fit for large businesses in this respect. This also allows workers to more easily work remotely as systems are no longer tied to internal networks thus freeing employees from the traditional desk-based PC. This will lead to less expenditure on office spaces and hardware. So, once you see the benefits of the cloud, you can see why most companies are moving there and hence why the hackers are targeting the cloud more [23, 24].

Before moving to a cloud-based system, it is necessary to understand the associated risks and benefits of cloud adoption. Data protection is important but is also a regulatory and legal requirement for law firms. With respect to cloud computing, the Data Protection Act requires that data must not be transferred to other countries without appropriate protection. It also prohibits the transfer of personal data to countries or regions outside European Economic Area, without adequate regulation in place [7]. For complying with the Data Protection Act, Cloud Service Providers are required to assure that servers used are within the EU or else comply with EU data protection laws. Before adoption, it is required that a risk-based assessment is done to ensure protection of the rights of subjects. Businesses will become more aware of only using proper cloud encryption techniques. This means they use disk encryption everywhere possible. Pre-Internet encryption (PIE)' should always be invoked in conjunction with whole disk encryption. This ensures that the cloud provider does not have the 'keys to a user's kingdom'. Strong encryption will be one of the key offerings by cloud providers in the short term. Of course, computation on the encrypted data in this case is not possible.

Businesses will have to pay more attention to cloud security as legal repercussions creep in and the increase in big data. Big data is generally cloud-based - private or public cloud. Therefore, all the recommended practices applicable to securing data in the cloud equally applies here. Companies should with large data sets due to the multi-tenant nature of a cloud platform pay extra attention to the data lifecycle phases and ensure that aspects such as data destruction is provided and auditable as part of the service. The fact that any company is allowing confidential datasets to reside outside the company network should lead them to examine how they can robustly protect that data and the answer can be simply a layered security strategy. The core principle to be followed here is the encryption of data.

Cloud-based file-sharing services like Dropbox and Evernote have signed "Safe harbour" agreements, which ensures that the client's data storage complies with the Data Protection Act. Nevertheless, the European Court of Justice states that businesses cannot rely on "Safe harbour" terms and should review the Service Level Agreement (SLA) by themselves to ensure data security [8]. The SLA not only details what services a CSP will provide but also addresses issues of data storage, control, and treatment. The desired level of service required is based on whether the data is stored in a public domain, where data centres are shared, or in private domain, where data centres are on-premise of an organisation [9]. The key features to look for in SLA document are: availability, support and maintenance, security, location and legal requests for data, portability, ownership, data centre locations and legal request for data. All businesses need to abide by data protection regulation, but law firms have additional obligation to protect their client's data confidentiality. This obligation to keep client data confidential is stated as Rule 4 of Solicitors Regulation Authority (SRA) handbook. The SRA has set of guidance for law firms on the use of cloud-based systems [10]. SRA states that the use of cloud computing can improve security in general however it does warn about the associated risks - "*Given the importance of legal privilege and client confidentiality, law firms should exclusively use established, known and, well-regarded cloud providers"* [10]. The SRA code of conduct identifies several risk factors such as loss of data control, confidentiality, integrity, and availability (CIA) in using cloud-based systems. The information security of cloud-based system rest on the classical CIA data principles, extensively applied to virtualised, distributed, and dynamic architectures [11].

IV. CHALLENGES IN CLOUD ADOPTION

Law firms are entrusted with client's personal and confidential data and any data breach not only causes financial implications but also the reputation and relationship with clients. When a law firm adopts cloud services, it implicitly trusts the CSP that manages the cloud. Therefore, it is essential to know what the main security challenges are and follow the best practices when choosing the cloud-computing platform [13]. Security of client confidential data, data privacy regulations and fear of handing over control are the three major cloud computing challenges [25]. The use of virtual machines (VM) in the cloud can provide more flexibility and computing power than the traditional servers. Even though the VMs are logically separated, all the VMs share the same hardware allowing data leaks and cross VM attacks [14]. Hypervisor vulnerabilities are another issue with cloud based VMs. The hypervisor is a key software component of virtualisation and is configured to meet an organisation's specific needs. As a result, a hypervisor can be exploited to take control of the underlying infrastructure. This manipulation allows the attacker to get access to the operating system referred to as VM escape and access to the other VMs residing on the same machine referred to as VM hopping [15]. Unrestricted allocation and deallocation of VMs and uncontrolled migration to balance load or fault tolerance can lead to data leakage [15]. Other data leakage risks are incomplete file transferring, processing, auditing, and storing the data [14]. Another challenge is data scavenging. Attackers may be able to recover deleted data as it may still reside on the machine

even though it was thought to be deleted. In cloud-based systems, it is an important that complete destruction of data is done, which includes destruction of log files and hidden backup registries [14].

When using a cloud infrastructure, distributed architectures, resource sharing, and VM synchronisation, more data is in transit. As a result, transit security is required to stand against man-in-the-middle attack, sniffing, and spoofing. Cloud computing use web-based interfaces to provide access to virtualised resources [14]. The attackers exploit the weakness of APIs to get access to the systems through account and service hijacking. As a result, the data can be manipulated, compromised, and redirected. Additionally, when the attacker has access to the system, Denial of Service (DoS) can occur [11]. With DoS, the services are disrupted, and the resources become unavailable to legitimate users [14]. Therefore, strong authentication mechanisms should be in place, such as multi-factor authentication, to provide robust authentication systems. Another challenge is governance and compliance, which addresses issues relating to losing administrative and security control when using cloud solutions. Migrating to cloud implies losing control over location, file systems and redundancy, and losing governance over security process and policies. This could happen when the terms and conditions are not clearly defined in an SLA, leading to security gaps, where client-side vulnerability assessment is not done [14]. Another issue is data redundancy and the CIA principles of mission critical data should be maintained at all the time to avoid any data loss.

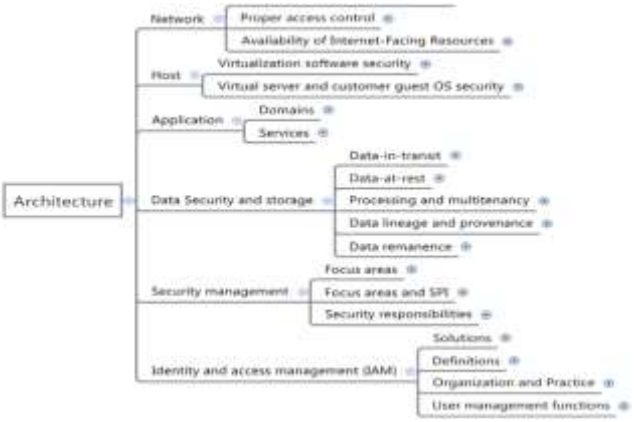

Figure 2: Cloud computing security issues in relation to *architecture* [14].

With the above analysis of security challenges, a comprehensive classification of cloud security is defined with three components as *architecture*, *compliance*, and *privacy* [14]. Figure 2 shows the *architecture* component of cloud security issues classification that includes hosts, virtualisation, network configuration issues, data security, and management of identities and access. The architectural component defines a clear division of responsibilities between CSP and client. Additionally, it provides an analysis of the kind of security role a CSP needs to play based on the nature of services provided such as software, platform, or infrastructure [14]. Next, the *compliance* component defines the administrative and legal responsibilities of a CSP towards the client. Figure 3 shows the *compliance* component of security issues classification.

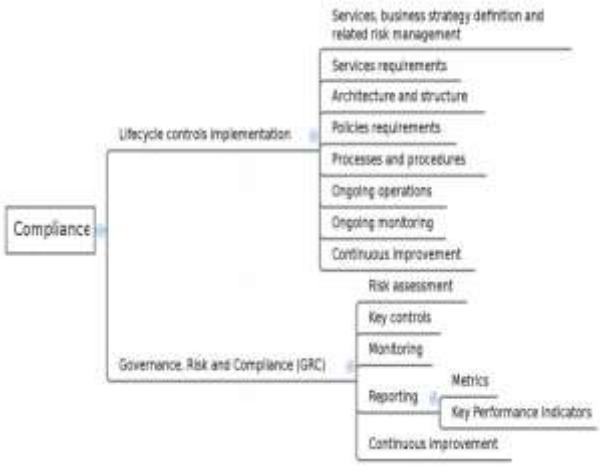

Figure 3: Cloud computing security issues in relation to *compliance* [14].

The *compliance* component is based on the cloud service lifecycle and governance. It defines issues relating to service availability and audit. The *privacy* component defines the client's concerns related to data and principles that a CSP should follow. Figure 4 shows the *privacy* component of security issues classification. The issues related to data generation, transforming, transferring, storing, using, archiving, auditing, and destroying is addressed in the concerns section of the *privacy* component. The best principles and practices to ensure data privacy, along with handling any personally identifiable information (PII) is also defined in the *privacy* component.

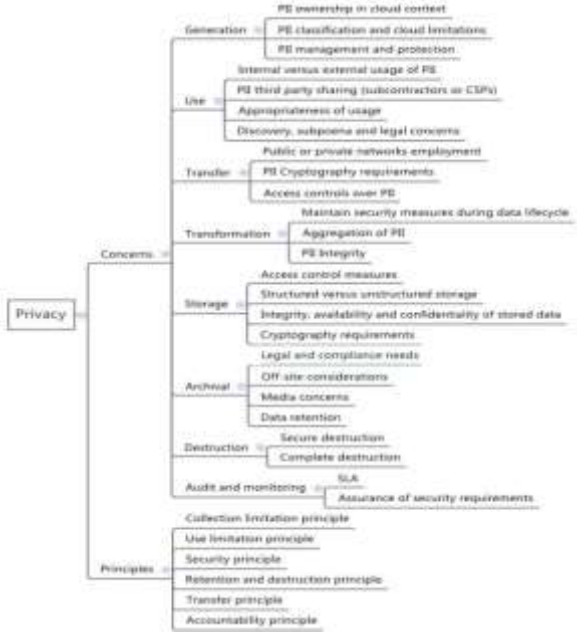

Figure 4: Cloud computing security issues in relation to *privacy* [14].

Both privacy and compliance need to be ensured at all the stages of data handling. To build a secure cloud storage

service, cryptographic techniques are deployed. The next section describes cryptographic cloud storage.

V. CRYPTOGRAPHIC CLOUD STORAGE

Data in the cloud has the risk of being modified or disclosed to unauthorised users. Therefore, it is essential that client data storage at rest and data transactions must be protected with robust secure practices. Cryptographic algorithms are used to accomplish secure storage in cloud [16]. The data before being uploaded on the cloud is encrypted and stored. The authorised user can decrypt the required data and download the file. Cryptographic cloud storage ensures confidentiality and integrity of the CIA data principles [11]. The data stored on the cloud service is encrypted, ensuring confidentiality and the encrypted data cannot be modified, therefore integrity is maintained. Data encryption transforms the plain data into another form that could be assessed using only a secret decryption key. The encrypted data is referred to as ciphertext and unencrypted data is referred to as plaintext. Regulatory compliance is maintained as the data is encrypted on-premise by the data processor(s) [16]. Standard Cloud security cannot guarantee the security of data during processing as the current limitations of cryptography prevent data from being processed in encrypted form. Given the fact that data is processed in unencrypted form, it is common for attackers to target data in use, rather than targeting data which is encrypted during storage or transit. This is where modern techniques such as Fully-Homomorphic Encryption, Oblivious RAM (ORAM) and Searchable encryption can play a role in the future of cloud systems.

Emerging techniques for cryptographic cloud storage

In the early days of cloud computing, public encryption keys were used for data encryption. Nevertheless, key management was an issue with simple encryption techniques as traditional encryption techniques cannot facilitate complex requirements such as fine-grained authorisation and query search on encrypted data [17]. Therefore, more advanced encryption techniques were required for cloud encryption. These approaches include the homomorphic encryption and searchable encryption.

Homomorphic Encryption (HE): HE is an encryption technique in which computation is possible on ciphertexts. The result of computation is a ciphertext which, when decrypted is the same as the result of the computation done on corresponding plaintexts [18]. HE permits the secure transmission and storage of confidential data on a cloud infrastructure; thus, allowing the use of different third-party services without exposing confidential data. There are two types of HE: fully HE (FHE), and somewhat HE (SWHE). FHE allows an unlimited number of computations on encrypted data without decrypting the data. FHE can be used to do searching without leaking sensitive data; however, FHE is very slow, making it inefficient to be implemented in the cloud. SWHE allows only a limited number of computations on encrypted data. As a result, HE is still not practical in real-world scenarios.

Oblivious RAM (ORAM) is a Client-Server communication protocol designed to obfuscate memory access patterns on the Server side of a given transaction. ORAM is also an effective cryptographic primitive developed to thwart access-pattern-based attacks in DRAM-based systems [26]. In the context of Searchable Encryption, ORAM is typically combined with SSE and PEKS Searchable Encryption schemes to improve their security. SSE and PEKS Searchable Encryption schemes Leak Information to the Server a few ways. By combining such schemes with ORAM, such Information Leakage can be eradicated; nonetheless, the search efficiency of schemes utilising ORAM is severely hindered due to the amount of work involved in obfuscating memory access patterns using ORAM.

Searchable encryption (SE): SE is an encryption technique that allows data to be shared privately while still allowing to do efficient search of limited type [19]. The string to be searched is first encrypted using the same key that was used to decrypt the original plaintext. SE encrypts a search string (search index or keyword) such that it contents are hidden except to authorized party that have access to relevant tokens. SE works on the assumption that a given term, either in plain format or encrypted format, resides at the same position in both the plaintext and the encrypted form of the same document [16]. The tokens are generated using a secret key. A search index generated for collection of files is encrypted such that: (a) given the token for a keyword (search index), pointers to the encrypted files that contain the keyword can be retrieved and (b) without a token, the contents of the index is hidden [16]. The retrieval process does not reveal any content of the encrypted files or the keywords.

However, after a set of searches, one can know about the files which have a keyword in common, thus leading to information leakage. The server can make certain assumptions about the client's search pattern and can use the information to guess about the keywords being searched for. This information leakage is not due to shortfall of the cryptographic technique but due to the way the service is used i.e. the keyword-based search [16]. In the case of Searchable Encryption, all associated keys are kept private. Searchable Encryption represents one of the few forms of Searchable Encryption that is achievable using standardized encryption algorithms. Alternative forms of Searchable Encryption require the use of non-standardized, special purpose encryption algorithms. Searchable Encryption is considered one of the least secure forms of Searchable Encryption primarily due to Information Leakage but solutions are available to eradicate and obfuscate all forms of Information Leakage in Searchable Encryption. However existing solutions have a significant effect on the search efficiency of Searchable Encryption. Evidently, the challenge for organisations is to improve the security of Searchable Encryption while maintaining its superior search efficiency. Searchable Encryption can allow cloud service provider customers like law firms to store their data in encrypted form, while retaining the ability to search that data without disclosing the associated decryption key(s) to CSPs [16].

It is to be noted that HE is for performing calculations on the encrypted data while Searchable Encryption is used for searching some key term in an encrypted document.

VI. CONCLUSION

Our relatively short modern Computing History to date has already shown us that organisations are not good at securing access in web facing portals so the decision to place such sensitive information on-line at this time is certainly interesting but increasingly becoming the defacto for storage of data due to perceived benefits and cost savings.

Developing secure, robust web applications in the cloud is hard. Any systems which provide externally facing data must be 'bullet proof' in their authentication mechanisms and have a myriad of other protections in place to stop the huge list of critical security risks to web applications.

Developers even those who do understand secure coding need to understand how to encrypt databases, prevent SQL injection attacks, know about third party library vulnerabilities, ensure passwords are hashed, implement multi-factor authentication, prevent denial of services attacks, ensure no resources are enumerable in the public API, do client-side input validation, know how configure cloud services, isolation of processes, use HSTS, uses IDSs, patch underlying virtual machines, restrict ports and ensure minimal access privileges. Hackers only need to find one flaw which allow them access while a legal firms systems administrator must ensure every known vulnerability is patched.

Cloud computing with its pay-per-use model allows firms to outsource their operations, allowing them to cut down the cost and virtualise their business. However, the law firms in comparison to other businesses have more obligation to ensure confidentiality and security of the operations such that the client data and trust is maintained at all the time. The major hurdles in cloud adoption by law firms are concerns about issues related to security and privacy. Keeping the Confidentiality, Integrity and Availability (CIA) data principles intact even when using cloud is the major issue when adopting to cloud.

We how described one exciting area of computing known as Homomorphic encryption which overcomes the limited capabilities of traditional cryptography, which did not support any computations capabilities in an encrypted domain. This was Searchable Encryption which can allow law firms to store their data in encrypted form, while retaining the ability to search that data without disclosing the associated decryption keys to cloud service providers.

Even though there are tangible benefits in cloud adoption, law firms should carefully investigate security measures when selecting a cloud service provider. Those selected should meet best practices internationally recognised in relation to rigorous enterprise security and control standards. Law firms need to understand data privacy regulations and data security implications when adopting cloud. Understanding challenges in cloud adoption in relation to architecture, compliance, and privacy is helpful for law firms to understand associated risks.

REFERENCES

[1] Anderson, C., Barahona, D (2017*) When "secure enough" isn't enough: A Law Firm Guide to Protecting the Confidentiality of Shared Client Files*. LexisNexis White Paper, https://www.americanbar.org/content/dam/aba/events/professional_responsibility/2015/May/Conference/Materials/4_byod_lexisnexis_document_security_whitepaper.authcheckdam.pdf

[2] Ponemon. (2012) *Confidential Documents at Risk Study*. Ponemon Institute LLC, July 2012, https://www.ponemon.org/local/upload/file/WatchDoxWhite_Paper_FINAL.pdf

[3] Bolin, R (2012) *Risky Mail: Concerns in Confidential Attorney-Client Email*. U. Cin. L. Rev.81 (2012): 601. https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.co.uk/&httpsredir=1&article=1003&context=ylas

[4] Eunjeong C. (2013) *How cloud computing is revolutionizing the future*. SERI Quarterly. 2013 Jul 1;6(3):104. http://www.seriworld.org/16/qt_PdfDown.html?mncd=0301&pub=20130321&seq=331

[5] CDW (2018) *Cloud computing and law firms*, White paper, https://webobjects.cdw.com/webobjects/media/pdf/Solutions/Legal/122223-White-Paper-Cloud-Computing-and-Law-Firms.pdf

[6] Cowhey, P. and Kleeman, M. (2012) *Unlocking the Benefits of Cloud Computing for Emerging Economies: A Policy Overview.* University of California San Diego. https://gps.ucsd.edu/_files/faculty/cowhey/cowhey_profile_10182012.pdf

[7] Bar Council (2015) *Cloud computing – security issues to consider,* The Information Technology Panel Report, The general council of the bar. https://www.barcouncil.org.uk/media/407878/cloud_computing.pdf

[8] Schneier, B. (2015) European Court of Justice Rules Against Safe Harbor. Schneier on Security, Ocotber 7th 2015, https://www.schneier.com/blog/archives/2015/10/european_court_.html

[9] Society, L. (2018) *Cloud Computing- Advice for the profession*, *Law Society of Scotland*. Available at: https://www.lawscot.org.uk/members/rules-and-guidance/rules-and-guidance/section-e/division-b/advice-and-information/cloud-computing-advice-for-the-profession

[10] Solicitors Regulation Authority (2013) *Silver Linings: cloud computing, law firms and risk,* Solictors Regulation Authority, November 2013 http://www.sra.org.uk/risk/resources/cloud-computing-law-firms-risk.page#executive-summary

[11] Wang, C., Wang, Q., Ren, K., Lou, W. (2010) *Privacy-preserving public auditing for data storage security in cloud*

computing, in Infocom, 2010 proceedings IEEE, pp. 1–9. DOI: 10.1109/INFCOM.2010.5462173 https://ieeexplore.ieee.org/document/5462173

[12] Khan, N. and Al-Yasiri, A. (2016) *Framework for cloud computing adoption: A road map for Smes to cloud migration*. arXiv 1601.01608 https://arxiv.org/abs/1306.2485

[13] Kenny, C. and Gordon, T. (2012) *Cloud computing issues for legal practices.* Law Society Journal. June 2012, http://www.olsc.nsw.gov.au/Documents/cldcomputing_lsj_article_june_2012_kenny_gordon.pdf

[14] Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M. and Pourzandi, M. (2012) *A quantitative analysis of current security concerns and solutions for cloud computing.* Journal of Cloud Computing: Advances, Systems and Applications, 1(1), p.11. https://ieeexplore.ieee.org/document/6133148

[15] Khan, N. and Al-Yasiri, A. (2016*) Identifying cloud security threats to strengthen cloud computing adoption framework.* Procedia Computer Science, Vol. 94, pp.485-490, https://doi.org/10.1016/j.procs.2016.08.075

[16] Kamara, S. and Lauter, K. (2010) *Cryptographic cloud storage*, International Conference on Financial Cryptography and Data Security, pp. 136–149. https://link.springer.com/chapter/10.1007/978-3-642-14992-4_13

[17] Sun, Y., Zhang, J., Xiong, Y., Zhu, G. (2014) *Data security and privacy in cloud computing*, International Journal of Distributed Sensor Networks. SAGE Publications Sage UK: London, England, 10(7), https://dx.doi.org/10.1155/2014/190903 https://www.researchgate.net/publication/274230804_Data_Security_and_Privacy_in_Cloud_Computing

[18] Ogburn, M., Turner, C. and Dahal, P. (2013) *Homomorphic encryption.* Procedia Computer Science, *20*, pp.502-509. https://doi.org/10.1016/j.procs.2013.09.310

[19] McBrearty, S., Farrelly, W. & Curran, K. (2017) *The Performance Cost of Preserving Data/Query Privacy Using Searchable Symmetric Encryption.* Security & Communication Networks, Vol. 9, No. 18, pp:5311–5332, https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1699

[20] Law Society (2017) *Fine or cloudy weather ahead? Cloud computing for law firms.* Law Society, 30 August 201, http://www.lawsociety.org.uk/news/blog/fine-or-cloudy-weather-ahead-cloud-computing-for-law-firms/

[21] Garrison, G., Kim, S., Wakefield, R. (2012) *Success Factors for Deploying Cloud Computing*, Vol. 55 (9), Pages 62-68, https://dl.acm.org/citation.cfm?id=2330685

[22] Layvas, J., Overly, M., and Karlyn, M. (2013) *Cloud Computing: A Practical Framework for Managing Cloud Computing Risk – Part II,* Intellectual Property & Technology Law Journal, Vol. 25 (4) pp.19-27. http://bciptf.org/wp-content/uploads/2013/02/Daniel-Carmeli-Cloud-Computing.pdf

[23] Vouk, M. (2008) *Cloud Computing – Issues, Research and Implementations*, Journal of Computing and Information Technology, 4 pp 235-246, DOI 10/2498/cit.1001391. https://hrcak.srce.hr/file/69202

[24] Helland, P. (2013) *Condos and Clouds*, Communications of the ACM, Vol. 56(1), Pp. 50-59 http://doi.org/10.1145/2398356.2398374

[25] Noor, T., Sheng, Q., Zeadally, S. and Yu, J. (2013) *Trust Management of Services in Cloud Environments: Obstacles and Solutions.* ACM Computing Surveys, Vol. 46 (1) pp.12-30. https://cs.adelaide.edu.au/~qsheng/papers/csur-2013.pdf

[26] Rakshit, J., Mohanram, K. (2018) LEO: Low Overhead Encryption ORAM for Non-Volatile Memories, IEEE Computer Architecture Letters, Vol. 17, No. 2, July-Dec 2018, DOI: 10.1109/LCA.2018.2795621 https://ieeexplore.ieee.org/document/8263412

[27] Mell, P., Grance, T. (2011) *The NIST Definition of Cloud Computing*. SP 800-145, September 2011 https://csrc.nist.gov/publications/detail/sp/800-145/final

[28] Bell, S. (2013) Titsup 2e2's data centre dustup gave UK users the CLOUD FEAR - Vendors struggling to reinflate the bubble. The Register, April 26th 2013 https://www.theregister.co.uk/2013/04/26/2e2_channel_fallout

This research was supported by the Ulster University Legal Innovation Centre. This centre provides research, development and educational resources for the promotion of innovation in legal services provision and access to justice.