University of Essex

Research Methods and Professional Practice January 2022

Research Proposal Presentation transcript

Project Title: Financial Institutions' Cybersecurity for Clouds and Datacentres

Introduction:

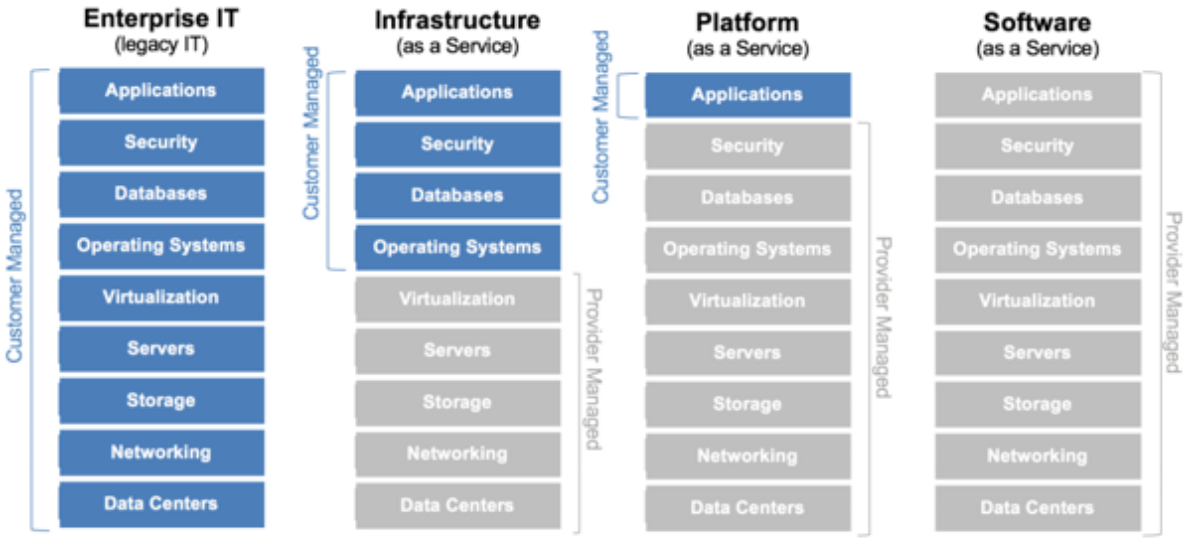
Cloud-based computing can offer substantial benefits for financial institutions and especially in risk management. However, some key challenges are migrating applications and systems between on-premises data centres and cloud-based. For many years, cloud computing was complex for financial institutions to obtain. However, the availability of cloud computing providers are better now, and users everywhere can have instant access to the computer's processing and storing capabilities. Many businesses have embraced cloud migrations as a risky change. However, it benefits them with the ability to process high data amounts, run new applications, and several benefits from more flexible and scalable technology. Banking has been slower than other sectors in adopting this kind of software; despite its potential, it is an area that needs significant improvement.

Cloud computing supports banks to make new markets and services to distinguish from competition and develop the ways customers' access and use the bank's products and services. (Asadi et al., 2017)

On the contrary, regulators warn of the risks of cloud computing by releasing guidance that highlights its effects on individual institutions and financial stability.

Significance/Contribution to the discipline/Research Problem:

The main difference between the cloud and the data centre is that a data centre refers to on-site hardware, whereas a cloud refers to off-site computing. The cloud stores its data in public areas, while the data centre stores its private information within its on-premises hardware. Therefore, migrating everything to the cloud is unnecessary when migrating from an on-premises data centre. Many enterprises have hybrid (on-premises and cloud) data centres that mix components of these two types of environments, which is the best solution for financial institutions' infrastructure architecture.



Managing cloud services (Bond, 2015)

The financial institution needs to have as much control over the cloud environments, which requires highly-skilled engineers from all technology departments. The engineers should architect the infrastructure by following the security standard written by the cybersecurity team. Security is one of the biggest arguments used against the actual cloud computing system.(Nedelcu et al. 2015)

Furthermore, there are critical requirements for the operation team to monitor all the live and critical business services to avoid any significant outages and lost money and customer trust. Usually, the cloud service provider is responsible for all security parts and makes sure all shared infrastructure are up-to-date. The engineers are likely working in cloud service providers more practising than the organisation's engineers as they take care of shared infrastructure for several customer containers.

However, there is one more critical part for financial institutions. It is for on-premises to cloud connectivity. Most companies use the internet to manage and connect to their cloud, but that is not secure. The best solution is to have a private circuit connecting the data centre to the cloud directly or at least use VPN(Virtual Private Network) to avoid any sniffing data. Amazon's VPC allows organizations to connect their existing legacy infrastructures to Amazon's clouds via a virtual private network (VPN) connection. (Sultan, 2010)

Research Question:

- What is the difference between a data centre and cloud computing?
- How does cloud computing help finance?
- Why do financial institutions use private cloud?
- Does public cloud secure for internet access?
- How to secure the cloud to datacentres connectivity?
- What are the benefits of data encryption?
- Can regulators and auditors allow financial institutions to store critical data in the cloud?

Aims and Objectives:

Cloud computing helps financial institutions host internet-facing applications outside the data centre and far from critical data. For example, most people like to use mobile or online banking to do any trading, bank transactions, pay bills, and more. However, financial institutions can use cloud computing for all website services, payment methods, news and targets, online services, and mobile applications.
What are the objectives and challenges of using cloud computing?
There are lots of objectives, but in the following some of them:

- **Scalability:** An on-premises data centre needs a long process and multiple departments to allocate new resources to the network or server when it is quicker in the cloud and meets business needs. Scalability is the ability of the cloud-based system to increase the capacity of the software service delivery. (Ahmad & Andras, 2019)
- **Availability:** in cloud computing, the availability is covered by the legal agreement contract with the cloud service provider, and in some situations, it is more guaranteed. When in the data centre, availability needs more in house resources and engineers.
- **Flexibility:** Cloud computing allows the employees and customers more flexible access by implementing the same service or application in different regions. This flexibility gives better experience and faster performance, especially for banks transaction.
- **Cost efficiency:** As cloud computing is a pay-as-you-go service, the financial institution can reduce the cost of operating and managing some of the infrastructure hosted in the cloud. The availability and scalability of cloud services are also financially unmatchable.(Liu & Yu, 2018)

There are several challenges to using cloud computing, like lack or loss of control over the system, audit and regulatory compliance, and the riskiest one is critical data privacy and how much is safe to keep in the cloud.

Key literature related to the project:

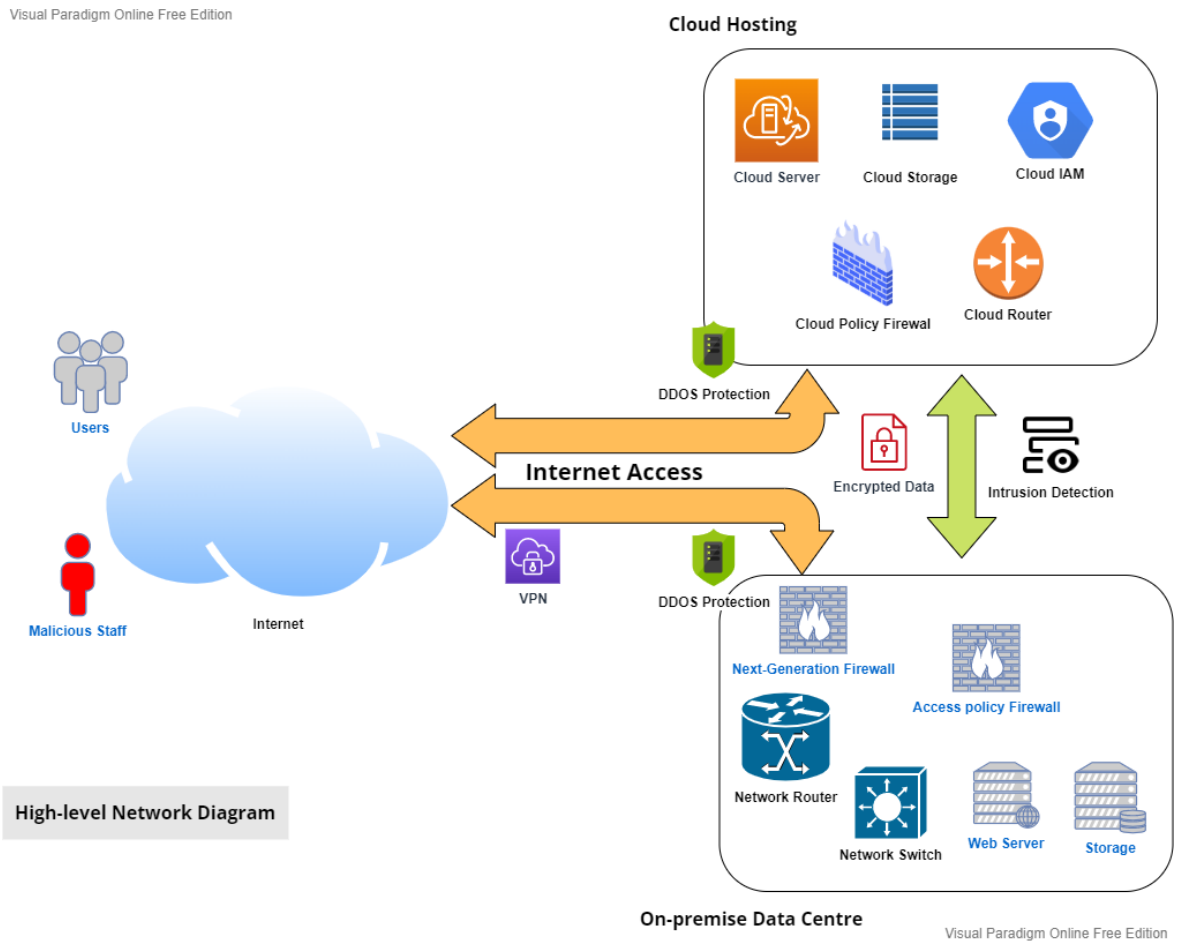
Customer and finance data, or what can be called Big data, is a significant asset for banks and financial institutions. Analysing big data helps to mitigate any operational risk and sometimes limit fraud. Depending on that, focusing on securing the data is a high priority.

- **Identity and Access Management (IAM):** It helps control the permission to access the critical data for customers, employees, and organisations. All significate data must be protected from cybersecurity attacks and data breaches. IAM policies manage the user's privileges and digital identities. Cloud IAM is more complex than traditional on-premises IAM since the user access is not defined to any geographical boundary or devices. (Irei, 2019)
- **Cloud computing secure connectivity:** In most data breach incidents, attackers try to steal the data by physical connection or sniff logical access. Using dedicated circuits or links for financial institutions will make the attackers' lives harder. As these types of connectivity do not have cryptographic protection by default, deploying it can provide high integrity and confidentiality. VPN or IPSEC tunnel is another type of connectivity, but it is not a stable choice.
- **Data protection** is also from most challenges for any organisation and not just banks. Companies should know where the data locations are and the security levels for the physical data centre. customers and providers must know and monitor where data is stored and used by cloud services, as the physical location of a provider's data center often does not correspond to the location of the provider's headquarters. (Russo et al. 2018)

Data Protection Framework (Sutherland, 2017)

- **Security incident management:** Managing cyber-attacks in a cloud environment is known as cloud incident response. The critical aspects of this system differ from those of a non-cloud incident response system, such as visibility and shared responsibility.

Methodology/Development strategy/Research Design:



High-level Network Diagram

The first concern about cloud security is the level of data protection. Of course, cloud service providers must follow the regulatory requirements for storing customer data. In addition, however, financial institutions must implement another level of security, especially for the cloud to on-premises connectivity.

Implementing strong security zones is very expensive for any company, but the finance and customer data are critical. The main security features are:

- Multiple firewalls level from different providers, standard firewalls check the source and destination with targeted application port, then deny the traffics not allowed by policies.

- Next-generation firewall for any internet-facing firewall, which inspects deeper in the packets and controls the application user access, intrusion prevention, detect any malware and leverages threat intelligence.

- Implement a DDoS solution to protect the incoming internet traffic from any threats or attacks. DDoS defence mechanism can be a combination of the following four phases: (1) prevention, (2) monitoring, (3) detection, and (4) mitigation. (Agrawal & Tapaswi, 2019)

- Implement Intrusion Detection systems with logging events to record and track any intrusion attack and meet the compliance standard.

- Encrypt the data travelling between the data centre and cloud, and find a robust encryption system for the data stored in the cloud to avoid the risk of stolen or hacking.

The business should invest in keeping the on-premises security infrastructure up-to-date and follow up with cloud service provider to make sure all cloud infrastructure meet the agreement.

Ethical considerations and risk assessment:

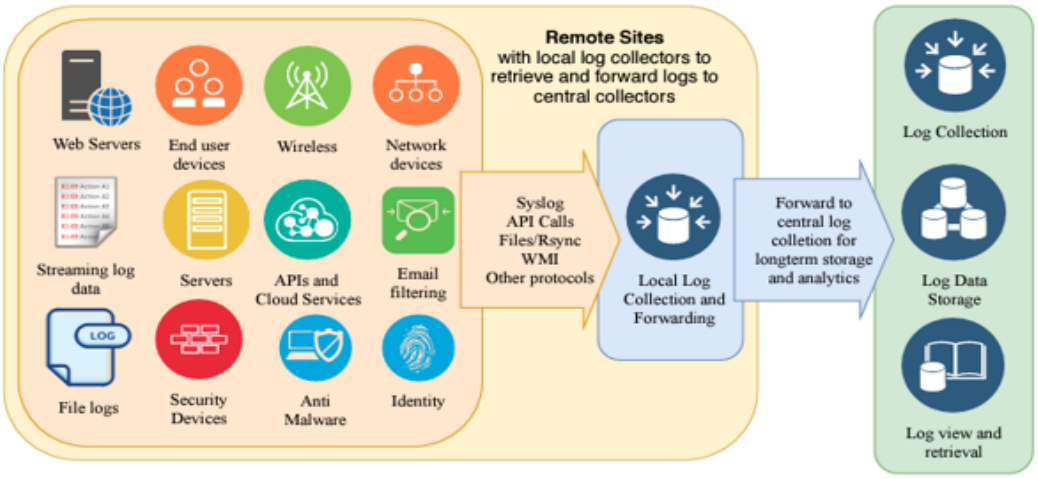
Financial institutions require risk management to ensure that they are not exposing themselves to various different types of risks. Accordingly, financial institutions need to manage these risks effectively in order to minimize the adverse effects on their performance.
For examples about the risks institutions:

- **Government regulations** can affect a company's ability to operate successfully depending on the type of market that a financial institution operates in and the number of active players. banks, more than any other business, face regulatory challenges due to the sensitive nature of their data. (Blazheski, 2016)
- **Operation risk**: It is the potential for financial losses resulting from a company not having adequate internal controls. Furthermore, it includes the risk of outages that could lose the business a significant amount of money. Cloud services are commonly inscribed with performance guarantees which play important role on cloud resource-management. (Herbst et al. 2016)
- **Regulatory and audit risks**: By violating regulations, Companies may lose their licenses, get fined by regulatory agencies, and have their charters revoked for violating regulations.

In order to mitigate various types of risk, financial institutions need to understand the risks to their business.

Logging and Monitoring System:

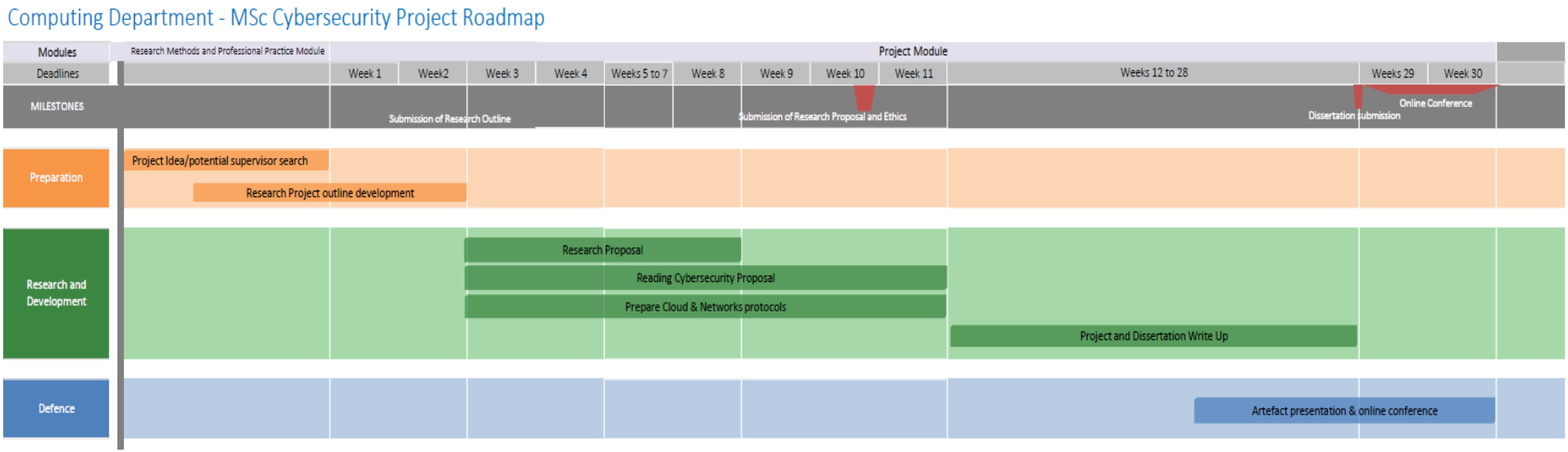
Logging and monitoring system is designed to provide information that allows businesses to manage and identify any become threats to the network. In addition, the system can collect the relevant activities that happen inside the infrastructure, including the firewalls, applications, systems, intrusion detection systems, and more. Logs can be collected through a number of mechanisms or protocols such as Syslog, SNMP, traffic flow, and more. (Onwubiko, 2015)
After data collection, the system starts to analyse it. Analysis of logs should focus on correlations, and filters must be set up for different use case scenarios to ensure that alerts can generate when data streams containing suspicious payloads are detected.
Next, the system should be monitored by the operation team. Again, there are various ways to monitor these items depending on the business needs or organisation strategy.
Finally, there should be a standardisation for any incident response depending on the security breach level.



Scalable log collection (Rehman, 2019)

Timeline of proposed activities:

The graph in this slide shows the timeline of the project roadmap. The first two weeks will start with the project outline, then the research and reading will begin with preparing for the cloud and network security protocols used in this project. Finally, starting week 12 to week 28, writing up the dissertation should be done to allow two weeks for the presentation and online conference.



Conclusion:

In the past, Financial institutions were slow to implement new technologies. However, many organizations are now embracing cloud computing to become more economical and effective at serving their customers' desires. Public clouds allow financial institutions, banks, and insurance companies to deploy financial services without needing infrastructure upgrades and maintenance.

In order to abide by legislation and regulation, financial institutions do their best to make sure that their IT infrastructure meets the requirements. In addition, they follow internal policies to ensure compliance with financial industry laws and regulations.

References:

- Asadi, S., Nilashi, M., Husin, A.R.C. and Yadegaridehkordi, E. (2017) Customers perspectives on adoption of cloud computing in banking sector. *Information Technology and Management*, *18*(4), pp.305-330. Availablr from: https://link.springer.com/article/10.1007/s10799-016-0270-8. [Accessed 26 March 2022].
- Bond, J. (2015) *The enterprise cloud: Best practices for transforming legacy IT*. " O'Reilly Media, Inc.". Available from : https://books.google.co.uk/books?hl=en&lr=&id=q_1xCQAAQBAJ&oi=fnd&pg=PR2&dq=The+Enterprise+Cloud+James+Bond&ots=poFI9xyTVJ&sig=lvHYO7loX8hP7J7yZu33mjN0gHY. [Accessed 26 March 2022]
- Nedelcu, B., Stefanet, M.E., Tamasescu, I.F., Tintoiu, S.E. and Vezeanu, A. (2015) Cloud computing and its challenges and benefits in the bank system. *Database Systems Journal*, *6*(1), pp.44-58. Available from: http://www.dbjournal.ro/archive/19/19_5.pdf. [Accessed 27 March 2022].
- Sultan, N. (2010) Cloud computing for education: A new dawn?. *International Journal of Information Management*, *30*(2), pp.109-116. Available from: https://www.sciencedirect.com/science/article/pii/S0268401209001170. [Accessed 27 March 2022].
- Liu, A. and Yu, T. (2018) Overview of cloud storage and architecture. *International Journal of Scientific & Technology Research*. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3649074. [Accessed 25 March 2022].
- Ahmad, A.A.S. and Andras, P. (2019) Scalability analysis comparisons of cloud-based software services. *Journal of Cloud Computing*, *8*(1), pp.1-17. Available from: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-019-0134-y. [Accessed 29 March 2022].
- Irei, A. (2019). New tech steers identity and access management evolution. Retrieved from https://www.techtarget.com/searchsecurity/feature/New-tech-steers-identity-and-access-management-evolution. [Accessed 23 March 2022].
- Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M. and Tosi, D. (2018) Cloud computing and the new EU general data protection regulation. *IEEE Cloud Computing*, *5*(6), pp.58-68. https://ieeexplore.ieee.org/abstract/document/8552651/ [Accessed 22 March 2022].
- Sutherland, A (2017) Data Protection and Cloud Computing Framework., Available from : http://architectureportal.org/data-protection-and-cloud-computing-framework. [Accessed 01 April 2022].
- Agrawal, N. and Tapaswi, S. (2019) Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications*

Surveys & Tutorials, *21*(4), pp.3769-3795. https://ieeexplore.ieee.org/abstract/document/8794618/ [Accessed 01 April 2022].

- Onwubiko, C. (2015) June. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-10). IEEE. https://ieeexplore.ieee.org/abstract/document/7166125/ [Accessed 30 March 2022].
- Rehman, R.U. (2019) Cybersecurity arm wrestling. *Building a modern SOC, Sisargo Pub*. Available from: https://rafeeqrehman.com/wp-content/uploads/2021/05/soc_book_20210404_first_edition.pdf [Accessed 30 March 2022].
- Blazheski, F. (2016) Cloud banking or banking in the clouds?. *BBVA Research*, *1*. https://www.bbvaresearch.com/wp-content/uploads/2016/04/Cloud_Banking_or_Banking_in_the_Clouds1.pdf [Accessed 31 March 2022].
- Herbst, N., Krebs, R., Oikonomou, G., Kousiouris, G., Evangelinou, A., Iosup, A. and Kounev, S. (2016) Ready for rain? A view from SPEC research on the future of cloud metrics. *arXiv preprint arXiv:1604.03470*. https://arxiv.org/abs/1604.03470 [Accessed 31 March 2022].