Al-Aqsa University Journal (Natural Sciences Series),Vol.24, No.1, Pages 40-59,Jan.2022
ISSN 2070-3155

Control Methods for Mitigating Critical Cloud Computing Issues in Banking Organizations: A review

Dr. **Abdelrafe Elzamly** [*]
Dr. **Nabil Messabia** [*]
Dr. **Hazem A. Elbaz** [*]
Dr. **Yunwei Yang** [*]
Dr. **Abdul Samad Shibghatullah** [*]

طرق التحكم للتخفيف من مشكلات الحوسبة السحابية الحرجة في المؤسسات المصرفية: مراجعة

الملخص

تُعرف الإجراءات والأساليب والتقنيات المستخدمة لتقليل مخاطر الحوسبة السحابية والتحكم فيها باسم إدارة مخاطر الحوسبة السحابية. يعد أمان السحابة مشكلة واسعة النطاق تشمل أي مجموعة من القواعد والتكنولوجيا وأساليب التحكم المستخدمة لحماية البيانات والبنية التحتية السحابية والخدمات ضد التهديدات المحتملة. الهدف من هذا البحث هو دراسة التقنيات والحلول لمعالجة مخاوف السحابة الرئيسية في المؤسسات المالية. علاوة على ذلك، تشير النتائج إلى أن أساليب التحكم في السحابة المستندة إلى البيانات الثانوية ستساعد في تقليل مشاكل الحوسبة السحابية. في الواقع، حددنا 20 أسلوبًا أساسيًا لإدارة السحابة للأعمال المصرفية لتقليل مشكلات السحابة، بما في ذلك أدوات البرامج الآلية المتكاملة، ومرونة السحابة، وقابلية التوسع السريع، من بين أمور أخرى. ستزداد احتمالية نجاح الحوسبة السحابية في الشركات المصرفية بشكل كبير إذا تم تطوير نماذج تحكم ناجحة تعتمد على أنظمة الحوسبة السحابية. في المستقبل، سنستخدم الذكاء الاصطناعي والاستراتيجيات المثلى لتقليل مخاوف السحابة الرئيسية باستخدام أساليب التحكم والحلول.

Abstract

The procedures, methods, and techniques used to reduce and control cloud computing risks are known as cloud computing risk management. Cloud security is a wide issue that encompasses any combination of rules, technology, and control techniques used to safeguard data, cloud infrastructure, and services against potential threats. The goal of this research is to examine techniques and solutions for addressing major cloud concerns in financial institutions. Furthermore, the findings suggest that cloud control approaches based on secondary data will help to reduce cloud computing problems. Indeed, we identified 20 essential cloud management techniques

Faculty of computer and information technology, Al-Aqsa University, Gaza, Palestine
[2]Département des Sciences Comptables, Université du Québec en Outaouais, Quebec (UQO), Canada
[4]Business school, Zhengzhou University, China
[5]UCSI University ,Cheras, Malaysia
E-mail: Abd_elzamly@alaqsa.edu.ps

for banking businesses to reduce cloud problems, including integrated automated software tools, cloud elasticity, and quick scalability, among others. The likelihood of cloud computing success in banking companies will be substantially increased if successful controlling models based on cloud computing systems are developed. In the future, we will employ artificial intelligence and optimal strategies to reduce major cloud concerns utilizing control methods and solutions.

Keywords: *Cloud Computing, Cloud Computing Issues, Cloud Control methods, Cloud Banking, Banking Organizations*

1- Introduction

Although cloud computing has many advantages, it is now plagued by security concerns. These days, the client's most pressing concern is security. If a customer wishes to fully benefit from cloud computing, the client's information, facilities, and applications must all be secure (Al-anzi, Yadav and Soni, 2014). While cloud computing has seen a lot of study and development, many cloud computing initiatives, particularly in the banking sector, have a high mistake rate(Elzamly *et al.*, 2015, 2017). Nonetheless, cloud technology has become a major focus for commercial businesses, which rely on cloud-based apps, storage capacity, and data centers, among other things. The impact of cloud technology on banks is significant and beneficial since it allows banks to be more flexible and effectively analyze and manage services(Sattiraju, Mohan and Mishra, 2013).

Cloud risk management has become a common practice among today's top financial institutions. Recent studies have identified a cloud computing hazard zone as part of the expanding effort to improve design practices and safety. Risk management helps corporate executives and teams to make more informed decisions about cloud computing risks. Cloud computing is a recently rapidly improved large-scale cloud computing technology that provides considerable processing and storage power by combining a large number of shared diverse assets (Yang, Wu and Yang, 2012). The term "cloud computing" refers to a concept of a computer network that can meet real-time user storage, processing power, and application demands. They define cloud computing as a system comprised of hardware, software, and processes that a user (in this example, an accounting department) may rent for real-time usage. Any department employee may access the scheme at any time using a variety of devices (PCs, laptops, mobile devices, etc) (Nikolopoulos and Tzouramanis, 2016). However, cloud computing is becoming a power in education, consumers are still concerned about security issues. Cloud protection challenges inhibit its use of cloud technologies for cloud users' privacy and confidentiality(Khalid & Zolkipli, 2022). Finally, the goal of our article is to regulate techniques and solutions for addressing important cloud concerns in financial companies.

2- Literature Review

Failures are frequently related to cloud computing. In the cloud computing life cycle, the risk of failure is defined as the chance of loss or exposure. Cloud computing risk management, in general, refers to the procedures, methods, and approaches that may be used to reduce the risk of cloud computing failure. Cloud security is a wide issue that includes any policy, technology, or control mechanism used to safeguard data, cloud systems, infrastructure, and services from potential assaults. Furthermore, previous studies concentrated on security technology rather than business factors like service stability, continuity, and availability (Gao *et al.*, 2013). Furthermore, the cloud bank

concept is an economic-based resource management approach. Its role in the deposit and lending sector is comparable to that of commercial banks (Li, Pu and Lu, 2012). SaaS providers who use cloud infrastructure have a number of possibilities. IT can choose between using their private cloud to mitigate risk and maintain control, using public cloud infrastructure, platform, or analytics services to further enhance scalability or implementing a hybrid model that combines private and public cloud resources and services based on workload, cost, security, and data interoperability(Sakharkar, Dande and Mate, 2017). Cloud computing is the technique of storing a large amount of data in order to retrieve it quickly in the future. Cloud computing is capable of more than just storage; it may also include a variety of security measures(Sen and Saluja, 2017). Cloud storage has grown in popularity due to a variety of advantages, including reduced storage management costs, open access with geographical independence, and the avoidance of capital expenditures on hardware, software, and personal maintenance, among others (Navya and Ramanjaiah, 2017). In the public sphere, cloud computing is gaining traction. Much of a bank or financial institution's operations take place with the use of technology, including through the Internet. Without solid cyber security measures in place, bank's sensitive data could be at risk. Banks and other finical institutions should understand how cyber criminals could invent complex new cyberattacks (Manoj, 2021). However, during the consultation phase, the following control mechanisms and cloud concerns for banking organizations flow diagram were proposed and refined: A PRISMA diagram for each review update, displaying simply the search results, screening, and inclusions for that update. The simplest method is to generate a distinct diagram for each review update; however, this would result in several diagrams when further updates are released, as seen in Figure 1.

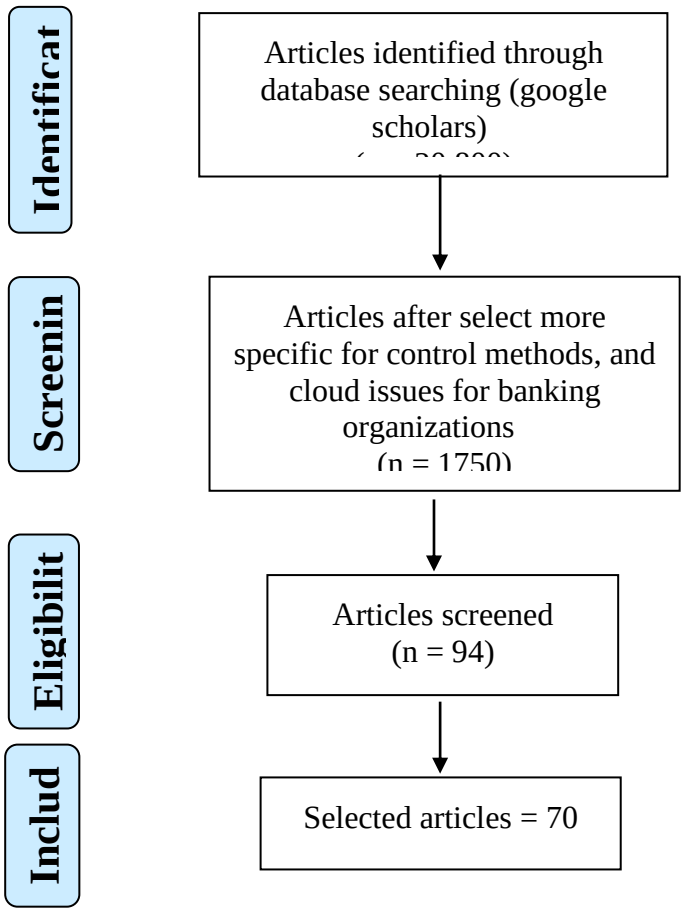
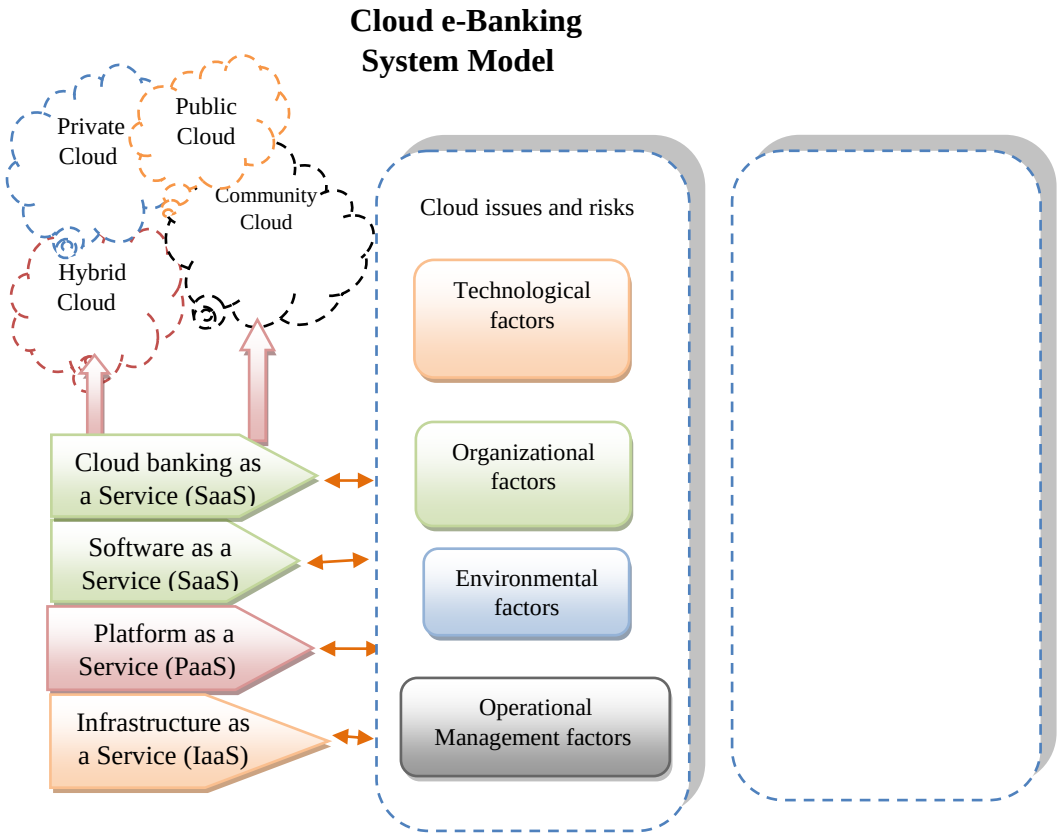


Figure 1 PRISMA flow diagram showing articles selection process

3- The Concepts of Cloud Modelling for Banking Organizations

In actuality, it was given with a cloud security service model and different modeling of information resources linked to virtualization security, multi-tenant security, and data security in service management procedures(Gao *et al.*, 2013). Although some security controls and techniques are tailored to each component of cloud computing, they want a framework that includes a quantitative risk management model. In the platform model, it offered risk assessment methodologies for determining cloud computing threats. Cloud users and suppliers can utilize the linear, iterative, and incremental technique to address and explain cloud dangers(Sendi and Cheriet, 2014). Cloud security is a vast topic, and any combination of procedures, strategies, and checks to protect data, infrastructure, and facilities from potential attacks or the attainment of corporate goals should work well across all security domains (Al-anzi, Yadav and Soni, 2014). To avoid software project failure, risk management methodologies and quantitative, intelligent procedures must be used in software development projects (A. Elzamly and Hussin, 2014a; Elzamly, Hussin and Salleh, 2015). One of the most critical challenges in providing a cloud computing service is the problem of security. It is critical for the cloud services company's success(Gao *et al.*, 2013). As indicated in Figure (2), we have separated the cloud computing model into four stages based on prior studies: cloud service models, cloud deployment models, cloud challenges and dangers, and cloud control security approaches.



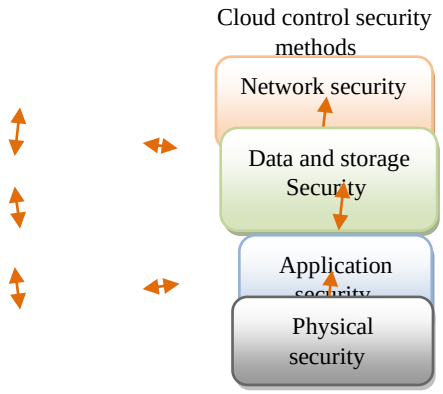


Figure 2 Adoption of Cloud Computing Model for e-Bank System(Elzamly et al., 2019)

3.1- Cloud Service Models

It one or more of four stages, each of the four forms of cloud computing can offer "on-demand" computation. The cloud service model is divided into four categories that may be accessed through a cloud provider: cloud banking process as a service (BPaaS), cloud software as a service (SaaS), cloud business platform as a service (PaaS), and cloud infrastructure as a service (IaaS) at different rates:

3.1.1- Cloud Banking Process as a Service

Organizations (for example, banks) that may provide commercial or financial services to their customers via mobile banking are considered business elements (e.g. mobile payments). With portable computers or technology, mobile banking apps may be provided(Gill, Bunker and Seltsikas, 2011). Mobile cloud computing is a new type of cloud computing that caters to mobile applications(Kaewpuang *et al.*, 2013). A mobile application (APP) is smartphone software that may be used on a mobile interface (Ho *et al.*, 2015). All virtual bank interaction points with clients, such as the internet and phone, were incorporated in the user interface. Due to the digital banking capabilities, banks and ATMs should not be considered customer channels (Ahmadalinejad and Hashemi, 2015). Mobile banking (MBanking) refers to any transaction involving banking services, such as checking a balance, making a bank transaction, making a deposit, or receiving SMS through a mobile device.

3.1.2- Software as a Service

The application level of Software as a Service (SaaS) is a paradigm in which software is introduced utilizing one of the four implementation systems. Users have no access to information or configurations and can only utilize software that is stored on the cloud(Arunkumar and Venkataraman., 2015). SaaS makes it easier for users to access apps and databases. The program does not need to be installed or run on the user's local computer. Because SaaS requires less maintenance, it is very cost-effective(Irfan *et al.*, 2015). The most popular approach is SaaS, which requires cloud providers to install and run the whole application stack on their platform, and customers access these apps directly using specific client software (Singh, 2017).

3.1.3- Platform as a Service

Clients develop their applications using the provider-supported programming languages and instruments on the Platform as a Service (PaaS) layer, which is accessed through an API (Beckers *et al.*, 2011). The customer is allowed to build apps that operate on the service provider's specific environment in the PaaS paradigm. To deploy your applications, the PaaS system provides infrastructure as well as complete operating and development environments(Goyal, 2014).

3.1.4- Infrastructure as a Service

In the Infrastructure as a Service concept, the service provider provides both digital and physical hardware as a service, with the entire infrastructure delivered through the internet. The client is more protected under this paradigm(Al-anzi, Yadav and Soni, 2014). IaaS provides clients with access to all equipment, including processing, storage, networking, and other major computing resources, as well as the ability to deploy and operate any software, including functioning devices and apps. Customers have no control over or regulation over cloud computing infrastructure, although they may change the operating system, storage space, and network parts within specified parameters(Wang, 2016).

3.2- Cloud Computing Deployment Models

The following are some examples of public, private, community, and hybrid cloud computing deployment models:

3.2.1- Public Cloud

Customers can access public cloud services through the internet via a third-party service provider(Irfan *et al.*, 2015). Because the term "public" does not always imply "free," employing public cloud services is also inexpensive when implementing solutions. Furthermore, the term "public cloud" does not indicate that there would be no security involved or that the information will be available to the whole public. The government can employ the public cloud, which is a cost-effective alternative for hosting apps. Google, Amazon, and Microsoft are three examples.

3.2.2- Community Cloud

In terms of the customer target set, a community cloud sits between public and private clouds. The Community Cloud intends to combine shared resources from grid computing, centralized control of digital ecosystems, and green computing development with cloud computing instances, enabling greater use of self-management advancements from autonomous computing(Goyal, 2014). This cloud infrastructure is managed by a group of businesses with similar concerns. It might potentially be governed by a third party(Irfan *et al.*, 2015).

3.2.3- Private Cloud

A private cloud provides amenities to a business via an intranet. To construct a buddy cloud, private clouds can be connected together. Private clouds are solely used by a single company (Beckers *et al.*, 2011). It is more flexible and dependable to design fine-grained access control systems to protect the privacy of financial information. On its private cloud, a hybrid may contain sensitive data and workflows and can provide the same level of security and privacy as a private cloud (Hu, Peng and Bai, 2015). A private cloud is housed in a company's data center and solely available to employees or associates of that organization (Goyal, 2014).

3.2.4- Hybrid Cloud

Hybrid cloud connects the strategic perspectives of public cloud services with the private cloud foundation, utilizing both government and private cloud techniques. In fact, the private cloud must be linked to the rest of the company's IT infrastructure and cannot be isolated from the public cloud (Alzahrani, Alalwan and Sarrab, 2014).

Critical Cloud Computing Issues for Banking Organizations

Cloud computing is a rapidly expanding technology that every business today aspires to incorporate into its operations in order to increase profitability and scalability. The properties of public, private, hybrid, and community cloud computation were covered in this letter, which introduced cloud computing and outlined all cloud computing business models (Goyal, 2014). The organization will be prepared to identify its vulnerability and power for each variable and then build and implement a strategy to help them make the best decision possible when it comes to cloud computing deployment (Al-shargabi and Sabri, 2016). In this section, you must handle the following critical security risks and challenges in cloud banking as technological, organizational, environmental, and operational management elements(Elzamly *et al.*, 2019). Cloud security is a vast topic, and any combination of procedures, strategies, and checks to protect information, infrastructure, and facilities from potential attacks or to fulfill business objectives should work well in all security domains (Al-anzi, Yadav and Soni, 2014).

5- Control methods for mitigating cloud issues in banking organization: Review

Cloud computing is another new technology that every organization wants to use in order to increase profitability and scalability. The purpose of this message was to explain cloud computing, highlight all cloud computing services, and cover public, private, hybrid, and community cloud computing (Al-shargabi and Sabri, 2016). Cloud security is a vast topic, and any combination of procedures, strategies, and checks to protect data, infrastructure, and facilities from potential attacks or the attainment of corporate goals should work well across all security domains (Al-anzi, Yadav and Soni, 2014). To avoid software project failure, risk management methodologies and quantitative, intelligent procedures must be used in software development projects (A. Elzamly and Hussin, 2014b; Elzamly, Hussin and ASH, 2016). One of the most critical challenges in providing a cloud computing service is the problem of security. It is critical for the cloud services company's success (Gao *et al.*, 2013). While risk cannot always be avoided, it may be managed in software development initiatives(Elzamly and Hussin, 2011; Abdelrafe Elzamly *et al.*, 2016). Cloud risk management is divided into several phases: cloud risk planning, cloud risk identification, cloud risk prioritization, cloud risk analysis, cloud risk evaluation, cloud risk treatment (RT) phase, which includes four approaches to dealing with cloud risks: cloud risk mitigation, cloud risk avoidance, cloud risk transfer, cloud risk elimination, cloud risk acceptance, cloud risk controlling (RC) phase, and cloud risk communication and documentation(Abdelrafe Elzamly and Hussin, 2014; Elzamly, Hussin and Salleh, 2015; Elzamly and Hussin, 2016a). In the meanwhile, any negative influence on an organization's purpose or business operations must be minimized by controlling the cloud computing environment that is employed as part of its information system(Kai *et al.*, 2012). However, in this part, we must emphasize cloud control approaches and solutions for financial businesses to prevent cloud issues:

5.1 Network security

5.1.1 Cloud Virtualization Technology and Virtual Machine

Virtualization technology is used by cloud providers to earn significant income. Virtualization is a major cloud computing technique that splits and shares physical resources(Khunger, Luthra and Bala, 2017). Virtualization technology is used in the cloud computing system to provide useful features such as resource abstraction and virtual machine migration. Cloud servers are hired on a pay-per-use basis by employing virtual instances. Virtualization of software is used by both physical network and cloud users. The core technology is cloud computing. Using the Virtual Machine (VM), virtualization allows you to run many servers on a single physical device (Alameen, 2017).

5.1.2 Using of Cryptography for Cloud Computing

The goal is to create incremental cryptographies that have applied the method to a text so that the results of the algorithm for a changed document may be promptly updated rather than having to recompute everything from the beginning(Yadav and Doke, 2016). Instead, then employing mask technology, it uses a cryptographic approach combined with bi-linear paring features to safeguard data privacy from auditors (Shajahan and Khasim, 2017).

5.1.3 Build Powerful Hypervisor Security to Control and Monitor the Cloud Activities

A hypervisor can be used to implement this technology. Cloud solutions are significant considerations when choosing a cloud product, and as a result, they support a variety of sophisticated hypervisors and virtualization types. Hypervisors of many varieties, such as VMware, Xen, KVM, and others, as well as host and bare-metal virtualization, can all be supported by cloud solutions (Arianyan, Ahmadi and Maleki, 2016). Hypervisors are software layers that connect different virtual computers to the underlying physical resources. Furthermore, operating systems can access these resources. Operating systems, on the other hand, may access hardware through this virtualization layer. Many commands were carried out by the software layer (hypervisor), which is not the most common technology, but virtual machinery(Yassein, Khamayseh and Hatamleh, 2016).

5.1.4 Best Practices for Measure Cloud Service Level Agreements

Cloud computing is a large-scale, interconnected computer built on Service-Level Agreements (SLAs) that is formed by consumer-service discussions with the supplier(Yassein, Khamayseh and Hatamleh, 2016). By defining the degree of compliance with cloud providers and agreeing on specific service level agreements (SLAs), data privacy may be safeguarded(Shanmugam and Tamilselvan, 2016). As a result, cloud resources must be distributed not just to meet the customers' QoS needs via Service Level Agreements (SLAs), but also to decrease energy usage (Taj and Basu, 2017).

5.1.5 Prevent Cloud Distributed Denial-of-Service (DDoS) attacks

DDoS attacks are a severe threat to cloud computing settings since they target the victim and completely disable the data center that is used by its legitimate customers(Ahamed and Iyengar, 2016). There are a number of cyber security concerns that may wreak havoc on cloud service availability. These attacks, such as Distributed Denial of Service (DDoS) attacks, are network-based(Bennasar *et al.*, 2017).

5.2 Data and storage Security

5.2.1 Enhancing Integrity and Privacy Data in Cloud Computing

The best way to safeguard data in the cloud is to use a combination of encryption, data loss prevention, integrity protection, authentication, and authorization approaches (Jakimoski, 2016). Because it is commonly known that data is kept in several data centers, the user is unaware of their exact location. Users are concerned that sensitive data might be stored on cloud servers because each country has its own set of rules(Sen and Saluja, 2017). The danger of privacy leakage and data misuse caused by remote storage, data manipulation, absence of service provider censorship, and an imperfect verification mechanism on user login checks are all part of the security issue. Users are not permitted to create data management standards or security measures for data that is in the control of service providers (Tao *et al.*, 2017). To avoid breaches of data integrity, privacy, secrecy, and availability, several laws and data protection measures were listed (Dhirani, Newe and Nizamani, 2016). It uses rules and policies to regulate who has the permission to do what in the cloud, protecting users' privacy and ensuring data integrity and confidentiality (B and Siddappa, 2016).

5.2.2 Predicting the impact of emerging regulations on strategic direction and business model

The storage of sensitive data on the cloud challenges regulatory compliance since different standards apply depending on where the data is kept (Elzamly and Hussin, 2016b). Each country has its own set of regulations and laws. This feature demonstrates how the cloud product may establish policies that are compliant with local laws and regulations (Arianyan, Ahmadi and Maleki, 2016). In addition, the firm may be able to store its data in select nations. Regulations do exist. When data is kept in a war- and disaster-prone region, the location of the data is equally important (Aldossary and Allen, 2016). Cloud computing is a new infrastructure paradigm that is rapidly gaining traction. By pooling processing and storage resources, the benefit is cost savings, which is paired with on-demand provisioning based on a pay-per-use business model(Kowselya and Aravind, 2017).

5.2.3 Flexible Access Control for Cloud Data Storage

Access control is a critical precaution when it comes to cloud computing data security. It guarantees that only authorized users have access to the cloud data that has been requested(Jakimoski, 2016). Access control is a critical precaution when it comes to cloud computing data security. It guarantees that only authorized users have access to the cloud data that has been requested(Arianyan, Ahmadi and Maleki, 2016). However, Cloud computing offers more flexibility than conventional computing methods, has more flexibility than other network

computing systems and saves time and money for busy and resource-less users (Tamzil et al., 2022).

5.2.4 Cyber security and Data Encryption

Another service that offers cloud data encryption is Cloud. Personal computers are allowed to encrypt data before sending it to the cloud. This level of security is exceptional since even the provider is unable to obtain the cost information(Jakimoski, 2016). From both the provider and subscriber sides, secure encryption techniques are often employed to ensure data integrity. Encryption, on the other hand, is one method of securely storing data in cloud computing. If the encryption keys are safe, it is impossible to decrypt encrypted data on its own to obtain the original data. At the same time, the encrypted data should be efficiently queried(Kantarcioglu and Ferrari, 2019).

5.2.5 Data Confidentiality and Audit-ability of Administrative Access

In addition, the Online Tech provider ensures secrecy by encrypting cloud computing data, which encrypts stored hard drive data during the procedure (like Full Disk Encryption). Encrypting data with the well-known AES (Advanced Encryption Standard) method is also possible with entire disk encryption. If a cloud-based device is lost or stolen, the data on the device is protected by a locker password. One of the most essential cloud data security methods for consumers is confidentiality. It comprises encrypting the plaintext before storing the data as ciphertext on the cloud. This method protects user data, and even cloud service providers are unable to change or access anything saved in the cloud using this method (Jakimoski, 2016).

5.3 Application security

5.3.1 Integrated automated software tools

They talked about the implementation/use of automatic version control tools which mitigate cloud computing risks(Elzamly and Hussin, 2015). Then there's cloud integrity, which relates to unlawful deletion, alteration, and theft protection. Simple data integrity maintains data integrity throughout transactions including data transmission, retrieval, and cloud storage (Yadav and Doke, 2016). In cloud computing, the term "automated tool" refers to the creation of information systems, methodologies, and automated tools(Nadanasundaram and Iyakutti, 2015).

5.3.2 Compliance and Risk Management Processes for Cloud Systems

In cloud computing risk management, the success of major financial businesses has become standard practice. Recent research has uncovered a danger associated with cloud computing, which has prompted increased attempts to strengthen development procedures and security. Risk management aids software project managers and teams in making better decisions on how to mitigate cloud risks(Elzamly, Hussin and ASH, 2016). Because risk management is involved in monitoring software success, identifying prospective hazards, and choosing what to do about the potential risk, it is viewed as planned risk control. It's a relatively recent occurrence to incorporate software engineering and product management into formal risk management (Elzamly and Hussin, 2016a). In terms of security and compliance, encryption, identity, authentication, and authorization, as well as data rights management, are extensively supported(Morin, Aubert and Gateau, 2012).

5.3.3 Developing effective authentication mechanisms and approaches for the cloud banking system

Authentication is the initial step of verification used to ensure that the appropriate services are being used by the right person (Singh and Singh, 2016). Cloud authentication guarantees that the data given by the cloud technology provider is only accessed by the appropriate business or person. When accessing information stored in the cloud, the user's identity is proven to the cloud service provider if authentication is assured (Jakimoski, 2016). The most essential items for the security technology evaluation, as well as supply chain management for security management, are authentication of identity procedures and solutions for data transfer (Ruo-xin *et al.*, 2014). Given the rise of hybrid cloud settings, interoperability for user authentication has also become a top need(Lim, Kiah and Ang, 2017).

5.3.4 Analytics and technology solutions to optimize compliance monitoring

Analytics, dynamic, and reactive algorithms for delivering resources and load allocation that heuristically maximize overall costs and reaction time while remaining compliant with major legal and regulatory criteria Cloud computing is a game-changing technology that improves collaboration, agility, scalability, and availability while also lowering costs through more efficient processing. They optimize the deployment and configuration of solutions for third-party rules, conformance, and risk management, such as Logical Apps (Major, 2019).

5.3.5 Application portability or interoperability

Furthermore, the more complex the applications and organizational data in a CSP cloud solution that uses proprietary tools grow, the more difficult it will be to change the provider(Alzahrani, Alalwan and Sarrab, 2014). Furthermore, the application portability of open-source technologies, platforms, and container technology makes it easier for businesses to switch cloud providers(Carr, PUJAZON and Vazquez, 2019).

5.4 Physical security

5.4.1 Security and Availability Architecture in Cloud Environments

A cloud computing system supports the distributary architecture as well as multi-user and multi-domain administration systems (A. Elzamly *et al.*, 2016). High cloud service availability can only help banks provide ongoing services with little downtime. The cloud may be configured to allow for near-real-time scaling(Ahuja, Mani and Zambrano, 2012).

5.4.2 Shared and Architecting Multi-tenant and Physical Security for Cloud Environments

In a multi-tenancy cloud, a group of users shares services offered by a single piece of software or application. Each mobile user's data is separated and inaccessible to other mobile users in this situation (Yadav and Doke, 2016). In this multi-tenant, resource pooling design, providing correct information and dynamic analysis is always a challenging challenge. However, if a computational model could establish trust, the system's security and privacy would undoubtedly increase dramatically(Shanmugam and Tamilselvan, 2016). Multitenancy is a critical cloud feature that allows resources like memory, applications, networks, and data to be shared among several users (Elzamly, Hussin and ASH, 2016). To win customers' trust, SaaS providers require a high level of security and a complex multi-tenant architecture(Bibi and Sumra, 2017).

5.4.3 Develop integrated risk strategies and frameworks across compliance, regulatory

In software teams, the Software Process Improvement (SPI) element is crucial for risk management. This provides us with a method for identifying and understanding dangerous zones in projects and strategies. It also aids in the comprehension of risk management in large organizations. Many methods and plans have been devised in order to accelerate the national deployment of cloud computing infrastructure and capture the cloud computing industry’s controlled height (Xiurong *et al.*, 2016).

5.4.4 Cloud Elasticity and Rapid Scalability

Rapid elasticity is a fast and automatic scalability supply, often with unlimited resources(Sasanapuri *et al.*, 2016). For high scalability, cloud computing refers to the utilization of

sophisticated virtualized resources that may be shared with end users. Without extra institutional investment, dynamic scalability adds the additional cloud computing processing buffer(Sasanapuri *et al.*, 2016). Scalability has tried to find better cloud databases that can handle workloads of any kind. A pay-per-use and elasticity database are the finest types of cloud databases. As previously said, huge data grows every day, and when the workload grows, a critical challenge for cloud databases arises (Ashraful Islam *et al.*, 2017).

5.4.5 Cost of Cloud management

In order for a business to stay effective, competitive, and successful, it must have secure and balanced access to information. Cloud computing provides a way to reduce resource access costs while also optimizing resource use. New software tools from faraway places are now available, eliminating the need for a costly resource(Sarddar, Sen and Sanyal, 2016). Cloud providers have started offering their surplus as low-cost transience servers, which can always be unilaterally revoked.

6 Conclusions

Although cloud computing has many advantages, it is now plagued by security concerns. These days, the client's most pressing concern is security. Cloud security is a wide issue that includes any policy, technology, or control technique used to safeguard data, cloud systems, infrastructure, and services from potential threats. The goal of this research is to examine techniques and solutions for dealing with significant cloud concerns in financial institutions. Furthermore, the findings suggest that cloud control approaches based on secondary data will minimize cloud computing problems. Indeed, we identified 20 essential cloud control approaches for banking businesses to mitigate cloud problems. Integration of automated software tools, cloud elasticity, and quick scalability, to name a few. A good cloud computing controlling model will substantially increase the likelihood of cloud computing success in financial businesses. We plan to develop a cloud banking framework in the future to combine control techniques and other components for growing financial businesses.

7 Acknowledgements

This project is performed as part of the Palestine-Quebec Science Bridge initiative. The authors also would like to thank Al-Aqsa University, Gaza, Palestine, University of Quebec Outaouais (UQO), Canada, and Palestine Academy for Science and Technology.

8 References

1. Ahamed, J. and Iyengar, N. (2016) "A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment," *International Journal of Security and Its Applications*, 10(8), pp. 277–294.
2. Ahmadalinejad, M. and Hashemi, S. (2015) "A National Model to Supervise on Virtual Banking Systems through the Bank 2 . 0 Approach," *ACSIJ Advances in Computer Science: an International Journal*, 4(1), pp. 83–93.
3. Ahuja, S., Mani, S. and Zambrano, J. (2012) "A Survey of the State of Cloud Computing in Healthcare," *Network and Communication Technologies*, 1(2), pp. 12–19. doi:10.5539/nct.v1n2p12.
4. Alameen, A. (2017) "Cloud Computing Data Breach," *International Journal of Computer Trends and Technology*, 47(1), pp. 42–49. doi:10.14445/22312803/ijctt-v47p105.
5. Al-anzi, F., Yadav, S. and Soni, J. (2014) "Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance," in *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, pp. 1–6.
6. Aldossary, S. and Allen, W. (2016) "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," *International Journal of Advanced Computer Science and Applications*, 7(4). doi:10.14569/ijacsa.2016.070464.
7. Al-shargabi, B. and Sabri, O. (2016) "A study of Adopting Cloud Computing from Enterprise Perspective using Delone and Mclean IS Success Model," *International Journal of Computer Science and Information Security (IJCSIS)*, 14 S1(February), p. 5500.
8. Alzahrani, A., Alalwan, N. and Sarrab, M. (2014) "Mobile Cloud Computing: Advantage, Disadvantage and Open Challenge," in *Proceedings of the 7th Euro American Conference on Telematics and Information Systems*, pp. 4–7.
9. Arianyan, E., Ahmadi, M. and Maleki, D. (2016) "A Novel Taxonomy and Comparison Method for Ranking Cloud Computing Software Products," *International Journal of Grid and Distributed Computing*, 9(3), pp. 173–190.
10. Arunkumar, G. and Venkataraman., N. (2015) "A Novel Approach to Address Interoperability Concern in Cloud Computing," in *Procedia Computer Science*. Elsevier Masson SAS, pp. 554–559. doi:10.1016/j.procs.2015.04.083.
11. Ashraful Islam, M. *et al.* (2017) "Architecture of DBMS as Integrated Cloud Service and Its Advantages & Disadvantages," *American Journal of Operations Management and Information Systems*, 2(16), pp. 37–41. doi:10.11648/j.ajomis.20170201.16.

12. B, S. and Siddappa, M. (2016) "A Novel Method of Designing and Implementation of Security Challenges in Data Transmission and Storage in Cloud Computing," *International Journal of Applied Engineering Research*, 11(4), pp. 2283–2286.
13. Beckers, K. *et al.* (2011) "Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing," in *2011 Sixth International Conference on Availability, Reliability and Security Pattern-Based*, pp. 327–333. doi:10.1109/ARES.2011.55.
14. Bennasar, H. *et al.* (2017) "Classification of Cloud Systems Cyber-security Threats and Solutions Directives," *Application and Theory of Computer Technology*, 2(3), p. 1. doi:10.22496/atct20170227147.
15. Bibi, G. and Sumra, I. (2017) "A Comprehensive Survey on E-Learning System in Cloud Computing Environment," *ENGINEERING SCIENCE AND TECHNOLOGY INTERNATIONAL RESEARCH JOURNAL*, 1(1), pp. 43–50.
16. Carr, B., PUJAZON, D. and Vazquez, J. (2019) *Cloud Computing in the Financial Sector*.
17. Dhirani, L.L., Newe, T. and Nizamani, S. (2016) "Tenant - Vendor and Third-Party Agreements for the Cloud : Considerations for Security Provision," *International Journal of Software Engineering and Its Applications*, 10(12), pp. 449–460.
18. Elzamly, A. *et al.* (2015) "Classification of Software Risks with Discriminant Analysis Techniques in Software planning Development Process," *International Journal of Advanced Science and Technology*, 81(2015), pp. 35–48.
19. Elzamly, A. *et al.* (2016) "A new conceptual framework modelling for cloud computing risk management in banking organizations," *International Journal of Grid and Distributed Computing*, 9(9). doi:10.14257/ijgdc.2016.9.9.13.
20. Elzamly, Abdelrafe *et al.* (2016) "Managing and Controlling Design Process Issues by Using Stepwise Approach Modelling," *Research Journal of Applied Sciences, Engineering and Technology*, 13(2), pp. 85–97. doi:10.19026/ISSN.
21. Elzamly, A. *et al.* (2017) "Predicting Critical Cloud Computing Security Issues using Artificial Neural Network (ANNs) Algorithms in Banking Organizations," *International Journal of Information Technology and Electrical Engineering*, 6(2), pp. 40–45.
22. Elzamly, A. *et al.* (2019) "Adoption of cloud computing model for managing e-banking system in banking organizations," *International Journal of Advanced Science and Technology*, 28(1), pp. 318–326.
23. Elzamly, A. and Hussin, B. (2011) "Estimating Quality-Affecting Risks in Software Projects," *International Management Review, American Scholars Press*, 7(2), pp. 66–83.

24. Elzamly, A. and Hussin, B. (2014a) "An enhancement of framework software risk management methodology for successful software development," *Journal of Theoretical and Applied Information Technology*, 62(2).
25. Elzamly, A. and Hussin, B. (2014b) "Evaluation of quantitative and mining techniques for reducing software maintenance risks," *Applied Mathematical Sciences*, 8(109–112), pp. 5533–5542. doi:10.12988/ams.2014.43206.
26. Elzamly, Abdelrafe and Hussin, B. (2014) "Identifying and Managing Software Project Risks with Proposed Fuzzy Regression Analysis Techniques : Maintenance Phase," in *2014 Conference on Management and Engineering (CME2014)*, pp. 1868–1881.
27. Elzamly, A. and Hussin, B. (2015) "Modelling and Evaluating Software Project Risks with Quantitative Analysis Techniques in Planning Software Development," *Journal of Computing and Information Technology*, 23(2), pp. 113–120.
28. Elzamly, A. and Hussin, B. (2016a) "Classification of critical cloud computing security issues for banking organizations: A cloud delphi study," *International Journal of Grid and Distributed Computing*, 9(8). doi:10.14257/ijgdc.2016.9.8.13.
29. Elzamly, A. and Hussin, B. (2016b) "Quantitative and intelligent risk models in risk management for constructing software development projects: A review," *International Journal of Software Engineering and its Applications*, 10(2). doi:10.14257/ijseia.2016.10.2.02.
30. Elzamly, A., Hussin, B. and ASH, B. (2016) "Classification of Critical Cloud Computing Security Issues for Banking Organizations: A Cloud Delphi Study," *International Journal of Grid and Distributed Computing*, 9(8), pp. 137–158.
31. Elzamly, A., Hussin, B. and Salleh, N. (2015) "Methodologies and Techniques in Software Risk Management Approach for Mitigating Risks: A Review," *Asian Journal of Mathematics and Computer Research*, 2(4), pp. 184–198.
32. Gao, Z. *et al.* (2013) "Management Process Based Cloud Service," in *International Conference on Cyberspace Technology (CCT 2013)*, pp. 278–281.
33. Gill, A., Bunker, D. and Seltsikas, P. (2011) "An Empirical Analysis of Cloud, Mobile, Social and Green Computing," in *An Empirical Analysis of Cloud, Mobile, Social and Green Computing*, pp. 698–705. doi:10.1109/DASC.2011.122.
34. Goyal, S. (2014) "Public vs Private vs Hybrid vs Community-Cloud Computing: A Critical Review," *International Journal of Computer Network and Information Security*, pp. 20–29. doi:10.5815/ijcnis.2014.03.03.

35. Ho, K.-F. *et al.* (2015) "Indoor Air Monitoring Platform and Personal Health Reporting System: Big Data Analytics for Public Health Research," in *2015 IEEE International Congress on Big Data*, pp. 309–312. doi:10.1109/BigDataCongress.2015.51.
36. Hu, Y., Peng, C. and Bai, G. (2015) "Sharing health data through hybrid cloud for self-management," in *2015 IEEE International Conference on Multimedia and Expo Workshops, ICMEW 2015*, p. 6. doi:10.1109/ICMEW.2015.7169752.
37. Irfan, M. *et al.* (2015) "A Critical Review of Security Threats in Cloud Computing," in *2015 3rd International Symposium on Computational and Business Intelligence (ISCBI)*, pp. 105–111. doi:10.1109/ISCBI.2015.26.
38. Jakimoski, K. (2016) "Security Techniques for Protecting Data in Cloud Computing," *International Journal of Grid and Distributed Computing*, 9(1), pp. 49–56.
39. Kaewpuang, R. *et al.* (2013) "A framework for cooperative resource management in mobile cloud computing," *IEEE Journal on Selected Areas in Communications*, pp. 2685–2700. doi:10.1109/JSAC.2013.131209.
40. Kai, S. *et al.* (2012) "Development of Qualification of Security Status Suitable for Cloud Computing System," in *Proceedings of the 4th international workshop on Security measurements and metrics - MetriSec '12*, p. 17. doi:10.1145/2372225.2372232.
41. Kantarcioglu, M. and Ferrari, E. (2019) "Research Challenges at the Intersection of Big Data, Security and Privacy," *Frontiers in Big Data*, 2(February), pp. 1–6. doi:10.3389/fdata.2019.00001.
42. Khalid, M.I.I. and Zolkipli, M.F. (2022) "Review on Cloud Security and Challenges on Higher Education," *MALAYSIAN JOURNAL OF APPLIED SCIENCES 2022*, 7(1), pp. 1–9.
43. Khunger, R., Luthra, P. and Bala, B. (2017) "EA Based Approach for Resource Allocation in Cloud Computing," *IJEDR*, (2), pp. 309–314.
44. Kowselya, G. and Aravind, T. (2017) "Reputation Attacks Detection for Effective Trust Management in Cloud Environment," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology ©*, 2(2), pp. 884–887.
45. Li, H., Pu, Y. and Lu, J. (2012) "A Cloud Computing Resource Pricing Strategy Research-based on Resource Swarm Algorithm," in *2012 International Conference on Computer Science and Service System*, pp. 2217–2222. doi:10.1109/CSSS.2012.551.
46. Lim, S., Kiah, M. and Ang, T. (2017) "Security Issues and Future Challenges of Cloud Service Authentication," *Acta Polytechnica Hungarica*, 14(2), pp. 69–89.
47. Major, A. (2019) *ERP Risk & Controls*.

48. Manoj, K.S. (2021) "Banks' Holistic Approach to Cyber Security: Tools to Mitigate Cyber Risk," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 12(1), pp. 902–910. doi:10.34218/IJARET.12.1.2021.082.
49. Morin, J.-H., Aubert, J. and Gateau, B. (2012) "Towards Cloud Computing SLA Risk Management: Issues and Challenges," in *45th Hawaii International Conference on System Sciences*, pp. 5509–5514. doi:10.1109/HICSS.2012.602.
50. Nadanasundaram, P. V and Iyakutti, K. (2015) "A Survey on Software Project Planning and Control Using Case Tools," *International Journal of Computer Science and Information Technologies*, 6(1), pp. 326–331.
51. Navya, T. and Ramanjaiah, G. (2017) "Protecting and Verifying Integrity of Cloud Data Regenerating Codes," *International Journal of Advanced Technology and Innovative Research*, 09(02), pp. 222–226.
52. Nikolopoulos, S.D. and Tzouramanis, N. (2016) "Data Mining Association Rules of ICT ' s Adoption Factors by Greek Accountants," *11th MIBES Conference – Heraklion, Crete, Greece*, 10(June), pp. 348–362.
53. Ruo-xin, Z. *et al.* (2014) "Model for cloud computing security assessment based on AHP and FCE," in *2014 9th International Conference on Computer Science & Education*, pp. 197–204. doi:10.1109/ICCSE.2014.6926454.
54. Sakharkar, V.S., Dande, M. and Mate, S. (2017) "Cloud and Big Data: A Compelling Combination," *IJESC*, 7(3), pp. 4867–4870.
55. Sarddar, D., Sen, P. and Sanyal, M.K. (2016) "Central Controller Framework for Mobile Cloud Computing," *International Journal of Grid and Distributed Computing*, 9(4), pp. 233–240.
56. Sasanapuri, C. *et al.* (2016) "Classification of APT ' s and Methodological Approach to Secure Cloud Services," *International Journal of Applied Engineering Research*, 11(2), pp. 1000–1005.
57. Sattiraju, G., Mohan, L. and Mishra, S. (2013) "IDRBT Community Cloud for Indian Banks," in *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1634–1639.
58. Sen, N.K. and Saluja, N.K. (2017) "Cloud Security Using Homomorphic Encryption.Pdf," *International Journal of Engineering, Management & Medical Research (IJEMMR)*, 3(4).
59. Sendi, A.S. and Cheriet, M. (2014) "Cloud Computing: A Risk Assessment Model," in *2014 IEEE International Conference on Cloud Engineering*, pp. 147–152. doi:10.1109/IC2E.2014.17.

60. Shajahan, Sk. and Khasim, Sd. (2017) "Guarantying and Verifying Integrity on Multi-Copy Cloud Data," *International Journal of Advanced Technology and Innovative Research*, 09(01), pp. 217–221.
61. Shanmugam, U. and Tamilselvan, L. (2016) "Dynamic Resource Monitoring of SaaS with Attestation for a Trusted Cloud Environment," *International Journal of Security and Its Applications*, 10(4), pp. 41–50.
62. Singh, N.K. (2017) "Advanced Security Model for Ensuring Complete Security in Cloud Architecture," *International Journal of Computational Intelligence Research*, 13(5), pp. 663–672.
63. Taj, N. and Basu, A. (2017) "Cloud Computing Security Issues and Challenges," *Imperial Journal of Interdisciplinary Research (IJIR)*, 3(1), pp. 1740–1745.
64. Tamzil, F., Anwar, N. and Hadi, M.A. (2022) "Security Utilization Of Cloud Computing In The World Of Business For Small Medium Enterprises (SMES)," *International Journal of Science, Technology & Management*, (2722–4015), pp. 41–49.
65. Tao, L. *et al.* (2017) "A Security Architecture Research Based on Roles," in *MATEC Web of Conferences*, pp. 1–7.
66. Wang, F. (2016) "Analysis on Safety-related Technology of Cloud Security in University Cloud Servicing," in *2016 International Conference on Wireless Communication and Network Engineering (WCNE 2016)*.
67. Xiurong, Z. *et al.* (2016) "Design and Implementation of Knowledge based Cloud Platform for NSFC Service System," *International Journal of Grid and Distributed Computing*, 9(9), pp. 171–180.
68. Yadav, D. and Doke, K. (2016) "Mobile Cloud Computing Issues and Solution Framework," *International Research Journal of Engineering and Technology (IRJET)*, 03(11), pp. 1115–1118.
69. Yang, Y., Wu, L. and Yang, S. (2012) "The structure of intelligent grid based on cloud computing and risk analysis," *2012 4th International Conference on Intelligent Human-Machine Systems and Cybernetics, IHMSC 2012*, 2, pp. 123–126. doi:10.1109/IHMSC.2012.126.
70. Yassein, M., Khamayseh, Y. and Hatamleh, A. (2016) "A Novel Technique for Jobs Scheduling in Cloud Computing Systems," *International Journal of Computer Science and Information Security (IJCSIS)*, 14(4), pp. 562–568.