Deep Science Publishing
https://doi.org/10.70593/978-93-49910-54-6_10

Chapter 10: Building scalable and secure tax administration infrastructure using cloud computing platforms

10.1. Introduction

Large, formal organizations are created to implement public policies chosen by the people through their representatives, including tax policies. Taxes represent a compelling share of any nation's gross domestic product. Therefore, ensuring a favorable environment for achieving tax compliance becomes vital for the economic health of any nation, especially when the efficiency of the tax administration is increasingly questioned by the representatives of the people. Modernity and civilization require that these large organizations operate efficiently and with the lowest possible cost to their citizens. Government tax agencies must put measures in place to make tax compliance more accessible and aid users to understand the tax code and comply with it, helping to avoid burdensome costs that do not represent a real benefit for society as a whole. These measures must be based on modern science and best practices in the area of public management. Currently, countries have a pool of feasible alternatives at their disposal, particularly information and communication technologies. The use of technology is essential to develop a good tax administration unit capable of securing mandatory payments required for the provision of public services by local, state, or federal governments (Alghofaili et al., 2021; Arvidsson & Hedman, 2021; Jain & Singh, 2023).

Despite a few exceptions, all countries use communications and information technology nowadays. Out of the several areas in which IT has been successfully implemented, the tax sector stands out, thanks to the convenience that both tax agencies and taxpayers take from the implementation of IT in tax-related tasks. However, only a few studies have tried to assess the influence of the degree of tax agency information on taxpayers' tax compliance. The aim of the present study is to analyze the influences and incentives that

a tax authority may provide to taxpayers through the informatization of tax services and the potential consequences of the availability of tax services on taxpayers' compliance with tax duties. This paper discusses how online tax compliance cross-border transactions information requested by tax authorities and sent by taxpayers, as well as cross-border transactions information received by taxpayers and sent to tax authorities influences the taxpayer's balance that favors tax compliance (Shukla & Mishra, 2020; Zinnbauer & Søreide, 2021).

10.1.1. Overview of the Study and Its Significance

A tax administration collects required revenue on behalf of the national government by acting for the benefit of society and citizens; hence, it is a part of required government service. If the electricity distribution service is not good enough, we can move on to gas or any other less important services in case we want to avoid any problems, but tax service is inevitable for the public. Specifically, the tax revenue collection process is a risky and sensitive task due to the essentiality and the nature of the process. Hence, we need a reliable service for collecting and maintaining this information. Apart from a small niche of taxes that remain cash based, tax compliance and enforcement become mostly electronic in nature by need.

It is true that there is a significant investment outlay for creating such supporting infrastructure; nevertheless, this area can still be considered an attractive opportunity for cloud service providers. Tax compliance and administration services are also the least sensitive of all government services when it comes to security and confidentiality. The information being submitted is much less sensitive than information being held by banks and financial institutions. Hence, it will not hurt the business case for cloud service providers, and governments of different developing countries will also get the benefit of scale from the services made available on the cloud. A working model for successful cloud deployment of tax administration services in developing economies has not yet been discussed. Filling this gap is the goal of this study.

10.2. Background and Rationale

In this chapter, we go deeper into the contexts of tax administration and cloud computing capabilities, presenting support arguments for the work subject. We present the more related works found in the area, emphasizing their particularities and the differences between our work and theirs, defining our position in the research scope. Finally, we present our research questions and the methodology we used to answer them.

Before addressing the problems that arose from the adoption of cloud computing in tax administration, let us outline the characteristics of a tax institution and what is usually expected from it. In the lowest level of a political federation, as a municipality, the tax institution would be responsible for collecting tax revenues, using them to provide social services to the collective, as public health, public security, public education, social assistance, urban infrastructure, etc., and for redistributing part of the collected taxes to the population, as a public safety net against natural disasters or risk from high economic cycles' volatility – a service that nobody would like to be without when necessary. In order for the tax institution to be able to provide those services, it must work effectively and efficiently, collecting enough resources to balance its operation with society's demands for better services and less payment for them. For that to happen, the tax institution model must be developed and adopted taking into consideration the particularities of the society in which the federation is inserted. The tax institution model, for the tax administration area, is represented by the good practices adopted by those institutions.

Tax institutions have been trusted for centuries by society's majorities to collect their resources so that the government may provide public services to their routines in a cost-efficient way. Reducing information asymmetry and convincing tax payers that the government is using tax revenues in a responsible way is key for tax institutions, with the ultimate aim of service delivery. Technology can help by providing service delivery channels, facilitating tax returns for service users. Tax institutions recognized the need to align their mission and strategic plan with the institutionalization of a broad electronic government strategy.

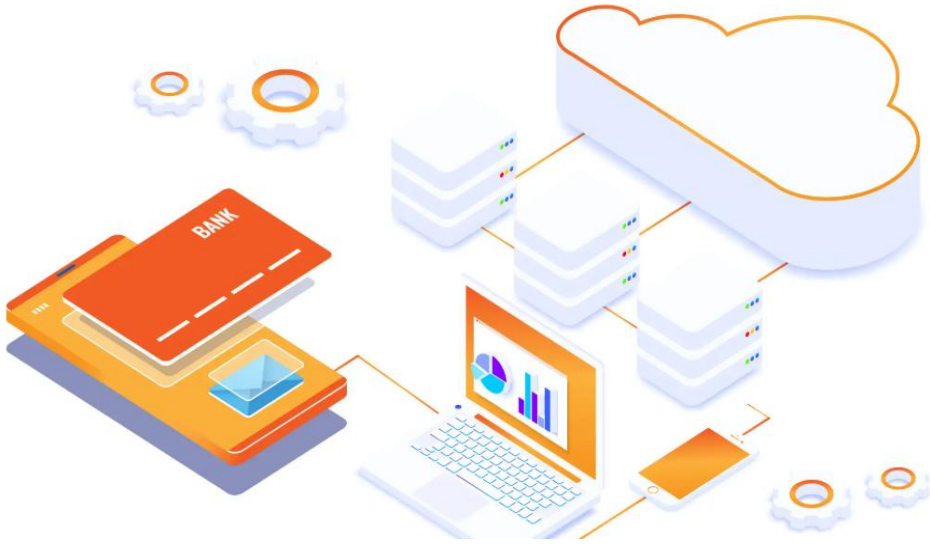

Fig 10.1 : tax administration infrastructure using cloud computing platforms

10.2.1. Justification for Cloud Adoption in Tax Administration

Cloud computing solutions and services are becoming increasingly used across sectors and levels of government. Cloud computing has the potential to manifest great benefits for any organization considering a transition from on-premises IT to a cloud infrastructure implementation. These benefits include: cost savings; good services and user experience with fast provision, development, replacement, upgrades, and scaling; maximized functions and greater security in information protection; more accurate data backup and recovery with cutting-edge tools; flexibility, portability and resource availability; increased collaboration and transmission efficiency for employees; supportive new implementations, hardware, and power option; increased efficiency and productivity; no need for internal storage; and technical assistance from cloud provider. Implementing a cloud solution requires a need for sharing infrastructure with others at the same time, while managing it with respective security, privacy, and risk mitigation solutions in order to fully maximize service benefits and advantages beyond those we can achieve with localized on-premises infrastructures. When these security, privacy, and risk mitigation considerations have been accommodated, performance in these associated areas can actually improve.

Transitioning to the cloud infrastructure - and especially a hybrid cloud model - allows leveraging functionalities and specializations from a unique cloud provider. For example, tax administrations can make use of auxiliary public sector units that have achieved advanced capabilities in information collection and management in order to access additional resources and abilities that would otherwise be very much time enfolding. All these benefits are also particularly relevant to capital-intensive and knowledge-dependent infrastructures, such as tax administration, usually facing severe fiscal constraints. Simplified budgetary processes supported by a commodities description of cloud services are a promise for exploring service prototypes long before order renewables, in a deploy-use-pay cycle that allows service value testing. Hybrid cloud models are usable, taking advantage of a unique specialization when tax information is sent and authority used only by tax administration systems.

10.3. Cloud Computing Fundamentals

1. Definition and Characteristics Cloud computing is an IT paradigm that provides rich services that include infrastructure, platform, applications, and consumer services to a number of heterogeneous clients using the internet protocol. Currently, cloud computing is being coined as the 22nd episode of the IT industry, which started from mainframe computing, and moved from desktop to network, and is now heading to the cloud. Cloud computing architecture consists of frontend and backend. The client side comprises a cloud computer and a network or cloud operating system, while the service provider side

comprises the network or cloud operating system and the storage system or cloud of data. The cloud of data is a combination of many data clouds. Cloud computing is relatively new, yet a very rapidly growing field. Its benefits depend strongly on the mode of adoption and the level of deployment. In contrast to several years back, when perceptions of the advantages and disadvantages of cloud computing were very uncertain, both private companies and governments are becoming more receptive to it. When done carefully, adopting cloud computing can help in cutting IT costs and/or improving agility. Though definitions of cloud computing can vary, generally it is viewed as any computing utilized to build, deploy, and deliver IT services, such as applications and development and testing environments in a more automated and efficient manner that are hosted by external service providers on the Internet. The services from cloud computing come from the combination of several existing technologies that have reached an adequate level of maturity and regulations and standardization that guarantees their safe usage. Cloud computing services can be grouped in three main service categories: Infrastructure as a Service, Platform as a Service, and Software as a Service.

10.3.1. Definition and Characteristics

Currently, the fastest growing trends in computer science are the adoption of distributed computing for scalable applications, and cloud computing, which makes use of distributed computing technologies for improving the deployability and cost-effectiveness of large applications. Cloud computing is a new technology enabling shared distributed processing of data stored in multiple servers. Through this technology, users utilize the shared processing power of computer networks on demand. Cloud computing enables on-demand access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing offers many prospects, including reduced costs, increased reliability and efficiency, and improved scalability and security. Many of these features have to do directly with cloud providers being able to afford much larger, more recent infrastructure, as well as being able to hire the best talent in many fields. There are three key characteristics that work together to provide the foundation of cloud computing. Resources are pooled – the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. This sharing of resources reduces the resources needed for each application and increases the utilization of the provider's resources. Customers don't have to invest in large-scale infrastructure and, consequently, can achieve a very low cost of ownership. Resources are virtually

inflated and available at any time. Resources such as processing power, bandwidth, and storage are available at any time and in any quantity to meet the demands of applications and customers. Cloud providers automate the process of making resources available. Customers don't need to request resources hours or days ahead. Thus, cloud computing is an ideal choice for enterprises with fluctuating workloads or unpredictable traffic spikes, because the infrastructure can easily scale up and down when needed.

10.3.2. Types of Cloud Services

Cloud computing provides a range of services that cover a myriad of use cases. The definition and guidelines bring a new vision to cloud services models by recognizing PaaS as a distinct service model, clarifying that cloud services may be used in multiple ways, such as automation and orchestration, while recognizing that some security responsibilities are explicitly shared between customers and service providers. Cloud services are broken into 3 models: Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS).

One of the most straightforward and widespread cloud services typology is the three-layer model made of SaaS, PaaS and IaaS. This typology grew up alongside the history of cloud services from a more infrastructure-led offering to application-led offering. SaaS is typically the first way cloud computing comes to the attention of the wider public. Hosted solutions accessible from a web browser are the original success stories of companies relying on the public cloud to deliver solutions without the complexities of installing, configuring, maintaining and updating software and associated hardware in-house.

The SaaS model removes the burden and costs associated with Hosting and Services Offerings for services such as Document Management, Expense Reports, Travel Management, Accounting, Sales force Management, HR management, Continuous Backup, etc. Companies can just connect to web-enabling Software Applications from anywhere in the world and get their work done seamlessly. The Web or the Internet, is the main channel of delivery for Hosted Software providers. They not only develop the software but also deploy and maintain it in their own physical infrastructure.

10.3.3. Deployment Models

The predominant deployment models for cloud computing environments include Private, Community, Public and Hybrid Cloud Deployment Models. The differing degrees of access to and transparency within the different deployment models are considered attributes of the models. A Private Cloud provides only a single business, or more

specifically, a single domain, i.e., core business process of business that is owned, managed, operated and hosted by an enterprise. Data and applications are not shared across domain boundaries but within that domain only. There are no other enterprise users or clients on the Private Cloud resources. It consists of a number of configurable resources dedicated to the domain. Private Clouds are also available hosted at a service provider location for a single enterprise. They might be further considered either Singleton Private Clouds if individual enterprise resources are not shared across domain boundaries or Shared Private Clouds if shared resources stored those enterprises. Enterprises using Shared Private Clouds would each be precluded from employing those shared resources for critical business processes, as a high degree of risk of performance degradation results from the lack of resource availability inherent in these cloud configurations.

A Community Cloud provides a partition of the Private Cloud, but operates in a manner similar to a Public Cloud. There are multiple enterprises within the community that allow their data and applications to be shared both technically and organizationally. Costs are thus shared among the members of the community and govern the level of service obtained. The Private Cloud can thus be considered the limit case of the Community Cloud where only one enterprise exists. In turn, the Community Cloud can be thought of as the limit case of the Public Cloud where all enterprises are actually the members of the community.

10.4. Tax Administration Challenges

The tax administration infrastructure currently being used is often inadequately developed, poorly designed, and in some cases, completely lacking. Furthermore, the current architecture built by tax authorities is often not in line with the rapid evolution of technology. Internal tax systems are not integrated with the business and other government systems to carry out certain operations. Moreover, in many low-income countries, tax authorities do not currently have the capacity to develop an efficient and effective tax system that relies on taxpayer compliance. Most tax infractions are committed by actors that are not easily recognizable or targetable by tax authorities. In addition, many tax agencies typically lack computerized tools for auditing all types of economic actors, and thus, do not take full advantage of the growing reliance by economic agents on e-commerce and digital transactions. The design of an effective plan for the development of a computerized tax administration and for its deployment must be carefully fitted to the legal system of the government and the degree of economic development of the country or countries involved.

Data security and privacy concerns are major impediments to removing the limits of taxpayer compliance, increasing the robustness of a computerized tax administration,

and optimizing its integration with the internal processes of taxpayers. Although new technological advances enable the design of systems and processes that can protect taxpayer data, secure digital transactions, and thereby raise levels of compliance, the need for mass data intrusions and e-signatures necessary to facilitate digital transactions that may be performed over and above the zero-intrusion limits of privacy standards must be formulated and accommodated so as to allow the process of seamless transactions to proceed in ways that are acceptable to society. The introduction of international legislation that outlaws intrusions must come as a priority to allow markets to cope with the major issue of taxpayer identification and authentication.

10.4.1. Current Infrastructure Limitations

There are inherent limitations in the existing tax administration infrastructure in Nigeria. The current tax system relies on unconnected and disparate IT applications for revenue collection. Operations across the tax agencies, both the primary Collector's office and the revenue agencies, which are more than 20 in number, are highly inefficient due mainly to non-integration of the various processes in the tax revenue collection. Many of these agencies still have manual processes, which adds to the risk of fraud. These applications are maintained and developed by consultants, which has resulted in a complex architecture with software solutions that are of limited usability across all agencies.

Tax administration in Nigeria is further complicated by the fact that various agencies have differing processes and, in some cases, different definitions of taxpayers. Each agency develops its own solution for a particular process in tax management and has completely different solutions for the same business problem. Although the government has mandated the different agencies to integrate with respective accounts in the Treasury Single Account maintained by the Central Bank, this has not translated into seamless management of the funds collected by the agencies.

The allocation of various tax types to different tax authorities adds to the challenges of tax administration in Nigeria. There are more than 50 different taxes chargeable by the three tiers of government. There is, for instance, dual collection of capital gains tax, which is an exclusive preserve of the federal government. The development of a singular and integrated tax system should include the establishment of a centralized taxpayer registry, which should tie all taxpayer identification numbers, VAT, TIN, agents ID into a single file. This will ensure that information from different agencies is linked into a single file and is updated whenever the taxpayer transacts taxable transactions with any of the government agencies. With a tax policy based on sound macroeconomic management and an integrated response to ongoing reforms, the problems of tax administration in Nigeria can be effectively addressed.

10.4.2. Data Security and Privacy Concerns

Most data in tax administration environments is highly sensitive. Among many types of related data are taxpayers personal profiles, such as the location or transactions amounts, payments information, declared income, properties owned, invested capital, legal entity's capital. Tax authorities often deal with hundreds of thousands or millions of individuals or legal entities in day to day operations. Cyber criminals are aware of this fact since tax authorities, financial institutions, and healthcare institutions hold the most valuable personal data. At the same time, the unauthorized disclosure of this data can cause very significant damage to individuals and legal entities. The total costs associated with identity theft could reach more than $50 billion. Additionally, the unauthorized disclosure of taxpayer personal data can cause reputational, financial, or operational damages at the tax authorities, leading to trust erosion.

Distributed Cloud services have difficulties in complying with certain regulations in terms of data localization, as the data may move from one region to another or from a private to a shared public infrastructure, often without the owner's awareness. Even more delicate is the unauthorized disclosure of sensitive or confidential data by authorized users. This type of breach is called an "insider threat". Performing a correct role assignment or a correct segregation of jobs and levels of authority is a very complex task, and Cloud computing makes it even more difficult since data is often processed by a community of Cloud service providers. Inside Cloud infrastructures, the tax administration data may be stored inside belonging to different companies, managed by specific Cloud software, and running on.

10.4.3. Scalability Issues

Scalability is one of the key characteristics of cloud computing, which allows various organizations to align their resource demand (CPU, memory, disk, and network) with the actual need of the organization at various intertemporal scales. In case of income tax administration infrastructure systems, during certain times of the year, a large number of taxpayers use the system, while during other months of the year, not many taxpayers submit their tax filings or pay taxes. Basically, during the peak period of this cycle, the requirement of resources from the income tax organization's perspective would be very high, while during the shoulders or off-peak periods of this cycle, the resource requirements would drastically reduce. With the current physical computing infrastructure-based systems used by the income tax department, tax resources would be always present, but often under-utilized, but in case of cloud data center infrastructure, resources can be added as the requirements ramp up, and they can be also released as demand dries up.

It is often said that one of the key performance measures of large cloud service providers is the ability to scale up and down seamlessly as per the fluctuations of demand, rather than being the absolute cost of the resources at a certain time of the day. However, it is important to note that tax administration-related processes are not immensely scalable by nature. Fiscal policy is only adjusted to smoothen out fluctuations in the economy and bring the economy close to its potential output levels. Tax collections, during downturns, are not generally a very big challenge because the economy is normally run by the private sector using its own resources. Tax policy does not have to be changed, but during upturns, one area where the government is often unable to keep pace is tax collection, which is controlled by government resources.

10.5. Advantages of Cloud Computing for Tax Administration

Tax administrations are information technology typically involved in tax collection, compliance, auditing, taxpayer assistance, and information security for the government. The infrastructure involved in conducting these activities is complex, requires much funding, and is highly intuitive. Hence, government departments need to ensure they make the right decisions so they do not risk losing sensitive information on their equipment. The cloud has become an attractive proposition for tax offices, as deploying and consuming services on the cloud becomes more convenient with the years. The idea of running automated tools that can optimize and prevent concerns about database availability and minimize downtime are goals in the cloud. The age of penalties is coming, so tax administrations are prone to discover new technology.

1. Cost Efficiency

Cloud computing can reduce a tax authority's IT costs by 30% to 50% compared with conventional deployment. These reductions hinge on the efficient use of cloud resources. When cloud resources lie unused, tax authorities linger for the potential benefits. With public clouds, external security concerns exist. However, tax agencies can initiate a private cloud internally for processes and data sensitive to security. The apparent upfront savings for tax administration from moving IT to the cloud are not only in equipment, power, and facilities but also in reduced operational overhead. Experts assume that 30% to 40% of the 1.2 million workers in tax agencies worldwide handle IT. Significant cutbacks in these support functions are possible through the operational flexibility of the cloud.

2. Improved Accessibility

Cloud computing allows authorized staff to access the tax administration's information at any time from any place in the world via the Internet. The taxpayers will also have improved accessibility to their account at any time, enabling such self-service

capabilities as making payments and requesting copies of returns and correspondence. In this way, tax administration can reduce the volume of calls to call centers and provide efficiencies in processing functions. Cloud computing can also improve accessibility through increased redundancies for the core applications. For example, accessible tax agency disaster recovery plans can enable key agency functions to be performed and taxpayer payments to be processed quickly even in a time of severe government data center disruption.

3. Enhanced Security Features

Proponents argue that cloud computing, especially commercial cloud computing and especially for smaller agencies, offers enhanced security features. Private cloud features are allowed, such as in the use of dedicated hardware and encryption. Commercial cloud vendors who have invested large resources in security features are implored. Cloud computing can also assist security through automated software security updates and redundant backups, which commercial cloud vendors and some tax administration private clouds can provide. In addition, dedicated staff is believed to be more quickly mobilized in case of security issues.

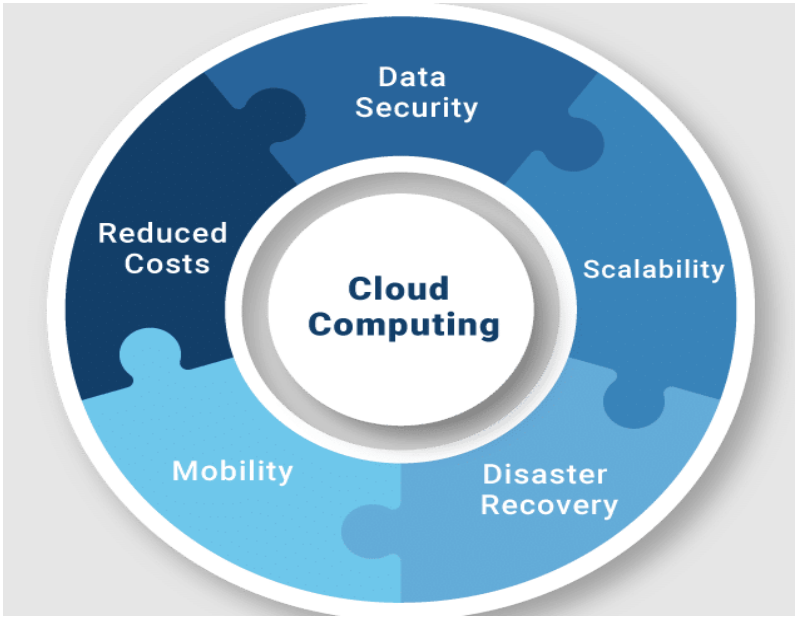

Fig 10.2 : Cloud Computing & advantages of Cloud Computing

10.5.1. Cost Efficiency

Cost efficiency is a crucial feature of cloud computing technology. Cloud computing can save money by significantly reducing costs for tax administration operations. Cloud

computing is low in initial costs because the cash outlay required to install disaster recovery resources like hardware and software is substantially reduced. The only expenditure needed is connection to the internet. Cloud computing can also cut costs associated with regularly maintaining the data storage facility. In addition, cloud tenants have access to cutting-edge hardware and software without incurring exorbitant costs, which is not possible when on-premises data storage is used. Cloud computing also reduces operational costs. Maintenance and testing of disaster recovery plans and procedures at the local level can be expensive. With cloud computing, however, the client only has to pay for what is used. Rather than overutilization to justify the costs associated with maintaining a local disaster recovery center, cloud computing is based on the economics of scale. With cloud computing, organizations can pay cloud service providers to store and protect data, applications, and IT resources. The cloud service provider can provide the storage at more advantageous pricing than the government because it can share resources among many clients. Cloud computing can eliminate the need for many experts to assign, install, maintain, and monitor an organization's disaster recovery systems. Hiring experts on a contract basis for cloud computing rather than on a payroll basis for on-premises data storage maximizes the return on investments. Cloud computing can eliminate risks and costs associated with the loss of mission-critical data because of an unforeseen disaster. Organizations can use cloud computing to keep data in a safe, off-site location so it is accessible even when the internal computer systems are temporarily incapacitated. Cloud computing eliminates costs associated with the loss of normal business service and the daily operations disrupted. This is important because down time after a disaster can expose IT organizations to loss of revenues and customers and reduced profits.

10.5.2. Improved Accessibility

Cloud computing offers improved access to software tools and data for use by civil servants, tax controllers, and third-party companies or consultants who assist tax agencies in their roles. Accessibility through mobile devices going beyond PC-based workstations serves to increase both information dissemination to more people, with higher skill levels, and also the inputs from citizens completing transactions at sales registers, using tax agency-developed apps, or visiting websites. Citizens using credit and debit cards for payments receive copies of transactions for their information. These papers become transaction-related records of tax compliance year after year. Transactions aid in the filing of annual tax returns by citizens for monitoring cheating, and enhance the overall efficiency of tax collection purposes. Communications via apps and the government's website are electronically documented. Sending alerts, reminders, notices, and other forms of communications to taxpayers can be easily programmed.

Those documents may be subpoenable should civic action relative to the obligations of a government agency arise. Because of the software support and oversight provided directly by the tax administration, the costs of such third-party support are highly reduced as there is less ambiguity in the rules to assist compliance efforts. If required, the software applications controlling transaction monitoring and documentation are programmed to ensure both government agency-required input and output should an agency employee perform a check of taxpayer compliance. Tax agencies can quickly respond to questions raised by citizens and taxpayers who have issues to be resolved, thus encouraging cooperation.

10.5.3. Enhanced Security Features

One of the primary concerns government organizations face is heightened security of their sensitive data, especially tax data. However, whether high security can be achieved is a critical decision that HCT arm faces before integrating cloud computing technology. A particular issue is that public cloud deployment forms do not allow particular organizations to privately operate their cloud; rather, such forms are particularly used by many tenants. This large sharing of resources makes public cloud infrastructures exposed to attacks, which can potentially cause severe consequences if a breach of sensitive information occurs. Addressing these concerns, many well-established cloud auditing schemes have recently proposed enabling the verification of the accuracy of the results of encrypted data returned from cloud computing servers, while ensuring the privacy of both the user data and the user query from data disclosure.

Existing cloud computing schemes either neglect to address the fine-grained data access control issue over the encrypted data returned from cloud servers or fail to guarantee either the integrity of the cloud service providers which are responsible to return the data search results over the encrypted data stored in the cloud, or the integrity of the encrypted data itself. Most existing models assume that the stored encrypted data and the cloud service provider service are trustworthy, the vast majority of existing cloud computing schemes simply utilize basic encryption mechanisms, and fail to provide fine-grained data access control to the cloud users who query via their encrypted keywords.

10.6. Designing a Cloud-Based Tax Administration System

The design of a CTAS must focus on its ability to provide all tax authorities' required services so they can efficiently and effectively carry out their assigned functions. Just like all other systems employed by a tax authority, a CTAS must be designed and built in accordance with the tax authority's policies, procedures, workflows and needs, so that it can assist the tax administration in providing services to its clients. The realization of

such design concepts depends on the careful selection of the appropriate infrastructure, whether on-premise, off-site, or a hybrid solution. Off-site services or hybrid solutions may be based on public, private or community clouds. Regardless of the chosen infrastructure solution, the CTAS design must minimize risks while maximizing service availability, security, simplicity, ease of use, ease of integration, and speed. CTAS designs based on community clouds that are managed by major tax authorities are an appealing and effective alternative.

Such CTAS design architecture must encompass all components of the cloud computing stack, from the physical and virtual IT resources, on which the other stack layers are built, to the applications that directly deliver services to the different tax authority departments. The management implementation must consider the specific nature of tax administrations and the sensitivity and confidentiality of all tax-related data residing on the cloud infrastructure. Attention must be given to system performance, design and responsiveness. Demand and capacity management tools must be employed to address situations of both high load and low load. Techniques like work caching, workflow management, server-side workload processing and load balancing can be used to effectively deal with peak loads.

10.6.1. System Architecture

Organization of tax and accounting data on a cloud-based system often can challenge scalability and privacy, availability, and data integrity. Public tax data set shown on the tax authority search page. Private tax data contains tax and credit information for individual taxpayers shown to him/her on the private tax web portal of the tax authority. This private tax data should be protected from malicious external attacks, while existing only for a few hundred of thousand domestic taxpayers, but it offers very high value on privacy policy with any legislative problem and attractiveness for malicious attackers. Tax data files can be very huge after dozens of data collection cycles, but occupy quite a bit of space on a periodic tax filing time, about one period of tax filing, from two to four months, in each year.

This paper proposes a cloud-based tax information system with system architecture. Cloud-based system infrastructure contains many servers to handle tax and tax regulation data periodically loaded from existing tax information system to prepare four types of tax services: new tax service requests; existing tax service requests; quarterly available tax information backup download requests; and the search requests to get general user help on the public tax data site for individual and corporate taxpayers. Main server with collective and periodical processing of incoming data services updated periodically, using other servers to redistribute such processing of the main server, and provide the available data for a few million user requests per hour compared with only

a few thousand requests for the existing tax information system. Tax information should be stored in databases on main server databases located inside the trusted area in the cloud to process such requests from taxpayers while the few systems should be independent without sharing cloud databases with tax information.

10.6.2. Data Management Strategies

A cloud-computing based tax administration solution requires a clear set of principles to produce a reliable, performative, secure, and maintainable system. In a cloud solution, we need to be very thoughtful about our data management strategy. For a number of reasons related to performance, maintainability, security, privacy, and legal considerations, we would like to ensure that certain data attributes are kept private, are encrypted at rest or in transit, are immutable once they are created, and that all created data is accessible, searchable, indexable, and reportable as needed, and that it supports secure authentic external queries. Additionally, since many state revenue agencies have to interact with other government agencies, it is preferable to have a common identifier across agencies.

In addition to addressing security and privacy concerns, data management has other consequences on reliability, performance, and system operating cost. One of the significant architectural properties of the cloud-based application design is to leverage the cloud's operational efficiencies. Data access is always the most costly part of a cloud application built using Infrastructure as Service or Platform as Service models. For a multi-tenant Software as Service model, the cost of data access can vary according to the data management strategy employed by the vendor. A common-chamber where all tenant data is stored and individual tenants can access data through a secure and audited process may be highly optimized for operational efficiency, but it may require a clause in the service agreement to ensure that sensitive data is processed according to the tenant's data policies. On the other extreme, individuals' databases and data storage solutions may be significantly more costly but would allow the tenants to comply with their privacy policies and regulations. It is imperative for all tenants to know about sensitive data attributes stored, and the put-in-and-pull-out process will require a shared empty payload.

10.6.3. Integration with Existing Systems

To enable successful integration, tax administration departments need to define standardized interfaces with mature and stable application programming interface specifications that all parties interfacing with or connecting to the cloud environment should comply with. Another key consideration is leveraging integration platforms as a

service that provides effective solutions that lower development costs and speed up integration efforts. This has enabled tax systems to simplify how tax systems interact with other internal and external systems. As part of their common set of services, import/export services should be provided for submitting and receiving file batches to/from the systems, standard national authentication and transaction acknowledgment functions, and standard APIs for file format validation, customer reference number validation, electronic acknowledgment, and currency format validation.

Most e-tax services are exposed commonly to banks and other third-party service providers. Other APIs are specific to products offered through third-party partners. If taxpayers are starting their business with a third-party service provider, they may need to register for opening the services either online or at the service provider's outlet. Selected taxpayers may also use the API to make tax payment through third-party partners that have made arrangements with the revenue department. For taxpayers who have existing government electronic tax payment query services, the new APIs allow the partners to offer payment statements tracking services to their customers. Using the other APIs, third-party partners can offer three additional tax services available in the cloud environment, such as e-tax service, e-withholding service, and e-collection service.

10.7. Security Considerations

Computing infrastructure security is a vastly growing concern nowadays. Various vendors are trying to address hundreds of vulnerabilities pertaining to IaaS and PaaS layers of cloud computing. Paranoid security experts would like to have tax administration IT infrastructure on-premises as there is a general bias that adoption of secure best-practice combination of virtualization, storage, and networking is hard. Although the IaaS cloud provides to us the basic building blocks of security, it depends on us how securely we design, implement, and utilize the services provided. Another very important contributor to IT infrastructure security is the wide set of data encryption techniques as well as access control mechanisms available in the PaaS layer. Security is also a concern of cloud vendors and they have invested extra efforts and costs to be compliant with the rules and regulations that have been enforced by regulatory and standard bodies. Reassurance can hence be taken that with adoption of the correct combination of security attributes for the IaaS and PaaS layers, the solution provides a sufficiently safe environment.

In this section, we will elaborate more about the security constructs and mechanisms specifically available in the IaaS and PaaS layers. We will also discuss some of the important cloud specific security developments and research that has emerged recently. As discussed before, an inherent concern with adopting the cloud for tax administration is the suspicion that the security levels of IaaS and PaaS layers are not up to standard.

As we have debated, as users of cloud services, we are provided the basic building blocks but then it is up to us as an organization to design, implement, and utilize their resources in a secure manner and also adopt a correct best-practice combination.

10.7.1. Data Encryption Techniques

The most important aspect of securing information in a cloud-based IT system is encrypting sensitive data in such a way that, inside the IT system, only authorized tax administration personnel can decrypt it. Each cloud computing provider has security requirements that the owner of the information system (tax administration in our case) can enforce on the provider. However, having such an agreement may not guarantee protection against snooping, even by the cloud computing provider, of sensitive information during its processing for purposes such as auditing or provision of legal services. This is because, in the service-oriented architecture of the information system, the data and processing are done by diverse service providing modules, with some of them possibly hosted on the provider's computing and storage resources. Therefore, employing a combination of both general encryption techniques and privacy-preserving encryption can minimize security vulnerabilities arising due to inappropriate management of tax sensitive information in public and hybrid cloud computing environments.

As for assigned services, non cloud computing facilities of the tax administration may want to use a different encryption algorithm and encryption keys than the assigned services in the cloud for the storage of sensitive tax data, as the cloud sites might be exposed to periodic physical inspection by the cloud provider. Advanced encryption techniques utilizing encryption keys that are changed at regular intervals should be employed, as the security of such schemes is guaranteed for a variety of probabilistically chosen values of plaintext and ciphertext. The encryption scheme may also include a known signature or tag, representative of the data owner's details, to verify the owner's authenticity when decrypting sensitive tax data.

10.7.2. Access Control Mechanisms

Modern cloud computing platforms provide various access control APIs and services, which allow user account records and access control lists to be created and maintained. Such services include various identity and access management solutions. Any organization using a cloud platform should not rely solely on the access control requirements and implementations provided by their cloud service provider. Organizations normally have additional log-in requirements and multi-factor authentication considerations that need to be coordinated with their cloud service

provider. They also may have unique requirements for the length and complexity of passwords that need to be coordinated with their cloud service provider. Furthermore, organizations should ensure that the auditing of administrative and privileged account activity is consistently reported for accounts stored in the cloud.

While detailed design and implementation of these cloud access control and protection services are beyond the scope of this text, some suggestions are outlined here. Organizations should expect their cloud service provider to comply with user management and logical access control processes and procedures that ensure that only authenticated users have access to cloud services and APIs. These processes and procedures should, at a minimum, enforce the principle of least privilege by providing granular permissions for resources, action, and data to provide users only the access they absolutely require, and have a process in place for controlling, managing, and auditing service accounts that access cloud services, which ensures that service accounts are provisioned with the minimum level of access for the job function, and are regularly reviewed to confirm their continued need. Automated business processes should be implemented to detect and respond to anomalous access activity.

10.7.3. Compliance with Regulations

Organizations that migrate sensitive data to the cloud need to keep in mind specific security requirements imposed by various industry and government regulations. For example, certain regulations require the protection of personal health information, restrict access to student education records, and mandate that federal agencies are responsible for securing sensitive user data. Achieving compliance with such regulations is a key challenge for cloud tenants, as the responsibility for compliance is likely shared. Some regulators release detailed compliance checklists to help organizations assess the compliance status.

Organizations may be further concerned about the compliance status of their cloud providers in case of a security breach. Subscription-based offerings are typically shared across multiple entities. A misconfiguration could mean that one organization can access another’s data. Third party auditing is one method for ensuring compliance with requests from regulators. It allows organizations to collect independent and objective assessments of their service provider's implementations and operating procedures, and helps organizations trust their service providers. Regular audits by independent third parties assess that specific control objectives are achieved and compliance is maintained for a certain period of time. However, organizations need a formal way to carry out audits in the cloud, as third parties no longer have unrestricted physical access to service providers' facilities and IT infrastructures. Auditing cloud services currently depends on service providers and their contractual agreements with customers. In some cases,

organizations have attempted to include contractual provisions that allow them to perform audits. However, in most cases, auditors rely upon security control assessments performed by external auditors on behalf of the cloud service provider, which is limited to a narrow scope and frequency.

10.8. Scalability Solutions

A tax administration solution must be scalable to satisfy increased workload during tax season. Tax management system workloads vary based on conditions, such as the actual submission date and the legal frame in place. This results in the tax submission timestamps distribution imbalance through the year. For example, declared tax value and the number of taxpayers vary from month to month but also depend on legal changes and announcements. This facet makes it a logical decision for tax management to design its own resources for satisfying upbeat demands and to rely on cloud services for offloading excess workloads. Because tax services are very sensitive and critical services, these excess workloads must be milder compared with other services, therefore additionally increasing costs during the non-tax season.

Ideally, resource provisioning would predict cloud environment dynamic behavior and deploy additional resources right before the increased load window and successfully release them when the workload drops down. Such predictions and deployment processes are very complex and difficult, therefore cloud services have developed elasticity services that are responsible for automated resource management. Elasticity solutions offer two major mechanisms, which are load balancer and autoscaling accelerator. Load balancers monitor the environment and react to changing loads by redirecting it towards the most available resources. Autoscaling accelerator, on the other hand, is a service that assesses the load coming towards the application and prepares it for the expected workload spikes. Based on application-specific information, the autoscaling accelerator can adjust the auto scaling configuration in order to optimize the time it takes to get to a steady state.

10.8.1. Elasticity in Cloud Environments

While Amazon Web Services is among the first cloud vendors to invent the concept of cloud elasticity, it does not mean that AWS elastic services alone are sufficient for an organization to realize the benefits from cloud elasticity. There are many other issues that need to be considered when building elastic environments. Some of the issues, such as elasticity monitoring, elasticity control, elasticity-friendly development, testing, and debugging tools, and so forth, would not be listed and described in this volume two, mainly because they would rely heavily on the unique use of workloads running on one

of these public cloud vendors. However, the other issues discussed in the chapter would provide techniques and strategies to help cloud service users to build their own application on top of AWS elastic services or other cloud vendor's elastic services in a way that can maximize the benefits for them from cloud elasticity.

Cloud elasticity, different from cloud scalability, refers to the ability of dynamically acquiring and releasing resources and service capabilities to meet fluctuating demand in the Internet-based scalable service environments. Compared to cloud scalability which traditionally is dependent on the capabilities of the workloads being serviced by the environment, cloud elasticity is mainly dependent on the fluctuation patterns of the workloads. That is, with the same environment, cloud elasticity can be achieved for one workload if it has significant periodic fluctuation, but not for the other workloads with the same resource usages or execution times that do not exhibit significant fluctuation. However, cloud elasticity could provide significant cost savings for services with workloads that return significant fluctuation. With cloud elasticity, for a highly dynamic bursty workload, smaller number of servers or resources plus around for the busy periods can be sufficient to meet the available or required performance, for example, response time or time-to-fit, during the busy periods, while at the same time, maximizing the available utilization levels of both the servers and the services during the idle intervals.

10.8.2. Load Balancing Techniques

Several approaches are used to provide load balancing techniques: dedicated software, hypervisor, and the switch. Dedicated software was the earliest load balancer technique. This method makes sure the request lines are balanced as evenly as possible at all times. It delays a small fraction of connections to fill up the emptiest link as the end requests compute for long and variable time. While this method produces the best performance, it consumes bandwidth in excess of some uniformly placed long transfers and distributed short pulls.

Each switch in a switched fabric is nonblocking and implements a round robin router to push packets fairly, but sending flows of different sizes through the same switch at the same time transmits none of the flows at the current best performance – larger flows do not get half of the switch capacity. So a load balancer should route a small flow through the switch with the emptiest nonblocking trunks and keep longer flows to go through just lightly loaded switches. As for virtual machine load balancing techniques, it was developed later as the concept of cloud computing emerged and has not gained widespread use while still in prototype. The hypervisors monitor the loads of the virtual machines running on them, assign VMs from the fastest balancing load by moving VMs to slower hypervisors at clean reuse checkpoints.

The preparation for balancing VM loads also maintains sufficient slack so some hypervisors can absorb the extra over a spot short surges – from users of distributed software or monitoring old circuit switching telephone networks for trouble clearing holes and plans. In these early systems, a changed management server would send the load balancer a number of spare VMs. The cloud then sends an unavailable response back to queues of users waiting for service, while monitoring for overcrowded systems, and clears each request queue. Cloud prepares for balancing firewalls and loads – the whole needed and sends a wireless push back so users can transfer packets elsewhere until the cloud service usability is made business hospitable again at the recommended time.

Fig 10.3 : Secrets From Cloud Computing's First Stage

10.8.3. Resource Optimization Strategies

Tax administrations' infrastructure on cloud computing platforms operates dynamically and experiences burst access patterns. Because of this, resource provisioning policies based on pre-defined thresholds may lead to high excess costs during periods of low activity, low quality of service levels during peaks and wasted capacity and resources. On the other hand, cost-optimal strategies that implement resource changes only periodically incur high excess costs during dynamic workloads with high peaks of activity. Hence, decisions on resource provisioning must factor the costs involved in invalidating pre-provisioned resources that still run during inactive periods. The cost of excess resources must be matched against the cost of invalidating stopped resources according to patterns of load change, degree of activity burst, volatility and

predictability. Non-diurnal tax-related workloads typically exhibit leaf patterns of load change that undermine the effectiveness of cost-optimal capacity provisioning strategies.

Non-diurnal workloads with burst activity patterns are usually submitted by enterprises that do their returns at the end of working hours on the last business day of a declaration period. Deferred-rate credit transfer requests, usually occurring in large batches, correspond to business hours, normally summer times in tropical countries, where companies or banks make deposits or refunds that involve tax administration. The voluntary acceptance by citizens of mandated behaviors supported by public policies usually create activity encore around signaling deadlines that exacerbate capacity problems on specific days for tax systems. These circumstances impose challenges on cloud based architectures for tax administrations to minimize idle costs but maximize availability or response time service-level agreements.

Consequently, specific management strategies must be implemented to allow economic use of infrastructure costs within which tax transactions run, regardless of the system's local times, while providing fault tolerance, redundancy and elasticity to traffic bursts whose potential economic impact on tax revenues justify the implementation of these measures. Tax system surveillance and monitoring are a key requirement for the establishment of resource provisioning policies that take into consideration scheduled volumes of tax or tax-related actions sufficient to justify the approximation of zero idle state costs for tax systems.

10.9. Conclusion

Recent years have seen the enactment of several initiatives, including in advanced economies, to establish the foundations of a data-centric generalized economy that promises to yield lasting benefits through increased productivity. These have been accompanied by a rapid transition to cloud computing platforms, which are playing the role of data infrastructure at the center of this new economy. Data on their own are little more than raw material, as is the case with other natural resources. In order to extract value from them, substantial investments in the development and deployment of the necessary technology must be made. The internet gave the world means to collect, process and distribute information at zero marginal costs. For emerging and developed economies, it is becoming an indispensable tool to provide affordable services at all levels, revolutionizing the provision of services through the combined use of electronic transactions, mobile devices and data analytics.

In this paper, we argue that, in order to reap the full benefits of the developments and opportunities offered by IT, emerging economies must design and deploy modern and efficient tax administration policies, ensuring its purchase and storage tax models for

digital transactions, as well as its electronic invoicing processes and their access to real-time transaction data, possibly stored in the cloud, allow them to cope with the new challenges at the tax policy, compliance and data governance fronts. Specifically, we illustrate how the core operations of tax administration can be modeled as a cloud computing system, which can be jointly developed by government and tax sector cloud service providers. By being enabled as cloud-native, tax administration systems can create massive software economies of scale that would render them sufficiently affordable for all economy participants to be operative, thereby allowing each of them to fully exploit the advantages of cloud-based services.

10.9.1. Final Thoughts and Future Directions

Cloud computing technologies provide the ability for tax authorities to become players in constructing and managing a government-wide tax platform. This section discusses future directions that enhance the ongoing government-wide reform initiative in which the tax domain is an integral participant. Although decisions are usually made by top decision makers and involve a host of government parties, we hope researchers and government practitioners can lead to deeper discussions on specific cloud items and encourage models on future directions. A continuous research effort involving working with data and providing simulations of models without significant implementations may not affect and encourage government leaders to pioneer and take risks on their problems.

Many advantages of cloud tax applications stem from increased data sharing. Data standards will need to be developed for tax authorities to effectively link to other government agencies. Increased usage of information from other agencies will lead to increased need by taxpayers for provision of information to tax administration. As increased data and processing capabilities become available, tax agencies will need to build and enhance their ability to leverage those abilities. These abilities include the ability to share data, the ability to use data for real-time decision making, and the ability to empower the data if non-government entities are providing data for tax administration. Enhanced data sharing will be needed to personalize data access and multiple multi-party data usage, such as onboard vehicle mileage tax, and to confirm general purpose revenue transfers. Data will also need security enhanced to ensure taxpayer data custody remains with non-government entities.

References

Zinnbauer, D., & Søreide, T. (2021). Cloud Computing for Tax Administration: Opportunities and Risks for Developing Countries. International Journal of Public

Administration in the Digital Age, 8(1), 12–28. https://doi.org/10.4018/IJPADA.2021010102

Shukla, S., & Mishra, A. (2020). Designing Secure and Scalable Tax Systems with Cloud Infrastructure: A Governance Perspective. Journal of Cloud Computing, 9(1), 47. https://doi.org/10.1186/s13677-020-00185-9

Jain, R., & Singh, P. (2023). Cloud-Enabled Tax Services: Strengthening Security and Scalability in E-Governance. Government Information Quarterly, 40(1), 101716. https://doi.org/10.1016/j.giq.2022.101716

Arvidsson, V., & Hedman, J. (2021). Digital Infrastructures in Public Finance: Cloud Strategies in Tax Agencies. Information Systems Journal, 31(3), 317–340. https://doi.org/10.1111/isj.12286

Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-Rimy, B. A. S. (2021). Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. *Applied Sciences*, *11*(19), 9005.