www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 8 Issue 12 December 2019, Page No. 24939-24952
ISSN: 2319-7242 DOI: 10.18535/ijecs/v8i12.4433

Cloud Security Challenges in Modernizing Insurance Operations with Multi-Tenant Architectures

[1]Sneha Singireddy, [2]Balaji Adusupalli

1. Masters, ORCID ID: 0009-0009-8450-5404
2. DevOps architect - Small commercial Insurance , ACE American Insurance, New Jersey, ORCID: 0009-0000-9127-9040

Abstract

Modern enterprises have embarked upon a tide of application modernization to leverage the promise of agility and lower costs in modern, cloud-based and multi-tenant architectures. While some application migration efforts focus only on a lift-and-shift approach, others contemplate bigger changes to take advantage of drastically newer technologies both in core business logic, as well as in supporting systems such as underwriting, claims, policy systems, etc. In this context, security considerations must permeate all aspects of the architecture, including secrecy, authentication, access control, accountability and audits, correctness, availability, data integrity, encryption, and loss prevention, logging security, network security, packet filtering, risk assessment, key management, certificates, storage security, system configuration, disaster recovery, attack tools, crypto, virtualization, firewalls, IDS/IPS, and zapping. Further, based on the challenges of security for multi-tenant architectures and of cloud security, we enumerate and describe the specific security recommendations to take into account while architecting multi-tenant architectures and note the gaps that cloud vendors offer.

From the perspective of the stakeholder's sweet spot, a multi-tenant architecture permits hosting entities to share devices, networks, and storage, gain economies of scale with lower costs, and efficiently service a large set of clients. Cloud offerings promise economies of scale as well as lower prices, allowing insurers to compete more effectively. Lower costs and speed of provisioning infrastructure allow smaller companies and start-ups to arise quickly and rapidly penetrate markets with innovative products. With a level playing field, insurers need differentiated product offerings to compete, enable innovation, and drive growth. At the same time, financial services are some of the most regulated industries, and insurers must be good stewards and protectors of their customers' most personal and sensitive data. Insurance companies have long invested in security infrastructure to protect themselves. The migration to the cloud for lower costs must not come at the expense of reduced data protection.

Keywords :Cloud security, insurance operations, modernization, multi-tenant architectures, data isolation, access control, regulatory compliance, tenant segmentation, identity management, encryption, shared responsibility model, threat detection, secure configuration, risk management, data privacy, scalability, governance, API security, policy enforcement, zero trust, monitoring, incident response, cloud-native security,

vulnerability management, compliance auditing, DevSecOps, cloud workload protection, security automation, third-party risk.

1. Introduction

Cloud computing is transforming many industries by lowering the cost of technology services and speeding their implementation; however, most organizations using these services are not aware of how sensitive and confidential their data really is and the specific risks they are exposing themselves to by utilizing commercial clouds. Insurance companies store massive amounts of extremely sensitive, personal information ranging from credit history and banking information to Social Security numbers. Besides the obvious risks originating from the vulnerability and exposure of personal information that cloud services can have on the individuals, insurance companies are also responsible for potential extensive financial losses from corporate theft and identity fraud, fraud, and property damage. As high performers, insurance organizations are subject to ever-expanding data regulation and compliance requirements. Keeping data compliance on-premises is a difficult enough task, moving some of that data to the cloud creates even more challenges.

Insurance companies have the dual responsibility of protecting invaluable information and complying with an ever-growing set of regulations on the personal data of their clients. While cloud service providers take on a large part of the security measures that are required to comply with many of those regulations, ultimately it is the organizations' responsibility to ensure that the necessary security protocols are in place to protect sensitive data from potential offenses. Unfortunately, with commercial cloud services, these organizations cannot always be certain of what those are or if they are being implemented. Properly planning the shift into cloud services requires a focused effort to identify not just the potential risks but also scalable and easy-to-implement ways to minimize those risks when moving to commercial cloud services.

2. Understanding Multi-Tenant Architectures

Multi-tenancy is a software architecture pattern in which a single instance of a software application serves multiple tenants. Each tenant is a group of users who share common access with specific privileges to the software instance. Multi-tenant systems are characterized by a single application and database that serve multiple tenant organizations, with the request routing to the appropriate tenant context. Multi-tenant architectures emerged on the heels of multi-user designs found in previously successful software packages. Multi-tenant architectures became practical for all commercial software packages with the commercial public network becoming the network of choice, followed by the release of the commercial application service provider approach. With multi-tenant architecture the design effort concentrates on building a single application instance that can be subdivided for use by different companies.

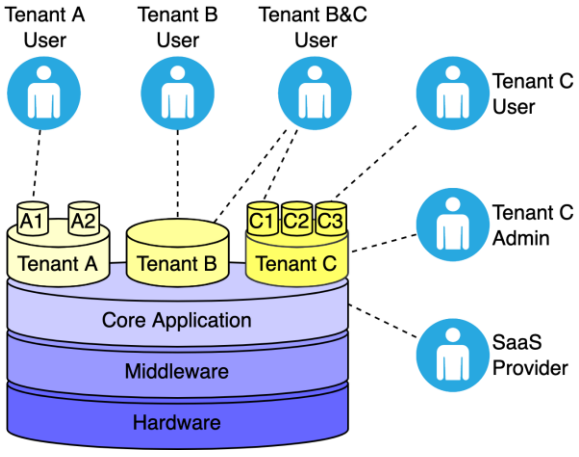

Fig 1 : Multi-Tenant Application. Software

Many multi-tenant applications exist in the SaaS and cloud computing realm. Even Flash-based games can be considered multi-tenant applications because they have many players customized for each. Building multi-tenant applications can be

easier than building single-tenant applications where each customer has their own custom application. However building the multi-tenant infrastructure that is flexible enough to support the variety of different companies and users using the application can be very difficult. Desktop software packaging was developed in the commercial realm and is easy as a result. The wide acceptance of the multi-tenant model for SaaS applications has made knowledge of how to build such applications priceless. A multi-tenant approach creates stronger economies of scale than single-tenant approaches. Economics of scale benefit from the use of a single backend. Companies save money on storage and processing on the same machine simultaneously.

3. Current Trends in Insurance Operations

Insurance is often described as the last bastion of verbal contracts between two parties, something that has changed considerably in the last couple of decades. While core principles still remain the same, insurance sales have become more technology focused. Instead of sitting down with a friend or neighbor, policy sales are now done over the phone, or with chatbots, often supplemented by artificial intelligence recommendations. What has also changed is how insurance companies manage their operations and provide services to partners, agents, and consumers. Modernization of back-office support functions has been the mainstay of enterprise support for decades, pioneered by development of enterprise resource planning, human capital management, and customer relationship management systems. Within this rapidly transforming industry, the demand for modernized core insurance operations is becoming painfully visible – antiquated, outdated, inflexible technology infrastructure that cannot flex and adapt to the demands of consumers, agents, and partners. Applications that talk to back-end systems are not going to cut it anymore.

Horizontal, vertically integrated ecosystems built around consumers, agents, and insurers are at the core of many insurance start-up companies that claim vast and disruptive improvements over incumbent insurance players along one or more segments of the omnichannel chain. However, even incumbent horizontal players, driving billions in policy sales, premiums, and profits, are hard-pressed to keep the lights on while also mining rich consumer insights from cross-channel interactions and data gatherings for digital transformation and use of predictive technologies such as data analytics, machine learning, and deep learning to enhance current processes or better manage fraud detection and other KPIs with latent values. Adding core policy management systems that are multi-tenanted and agile onto a modern enterprise services backbone then becomes critical for the entire insurance industry.

4. Key Security Challenges in Multi-Tenant Environments

Security is a fundamental concern for any cloud computing environment, yet it becomes especially challenging in a multi-tenant architecture. Understanding these security challenges helps both providers and customers make small adjustments to their operation and usage models that can greatly improve the overall security of cloud-based operations. Cloud security challenges include data isolation and privacy, access control, and compliance issues, specifically for the insurance industry. In this section, we analyze these challenges and discuss their implications. Even though cloud computing services are designed to provide isolation between tenants in a multitenant architecture, it is extremely easy to ignore architectural aspects of the multitenant design and inadvertently break this isolation model. Because of the complexities involved in a multi-tenant deployment model, risks also may be higher than that of non-multi-tenant models. The primary risk is that one group of tenants can access the information of another tenant. In data control for commercial applications, this risk is amplified for sensitive data, which for insurance applications includes the personal and medical records of customers being

protected by laws. Sensitive data typically includes names, addresses, dates of birth, records of medical treatment, and other identifying information.

Fig 2 : Top Multi-Tenancy Testing Challenges

4.1. Data Isolation and Privacy

Since insurance operations are moving to the cloud, are beginning to work more and more with sensitive data, and are also beginning to collaborate with other domains, data privacy and confidentiality will always be a big issue in insurance, especially in multi-tenants domain. Privacy and data separation must be enforced and guaranteed by the cloud provider. Such requirements, however, are not easy to be satisfied in a multi-tenants cloud scenario. A lot of questions arise in this security area: how is users' data securely separated in the cloud provider's storage devices? How does the cloud provider guarantee data privacy of my data? What if it is misused or disclosed, even just inadvertently, to other users? What kind of algorithms does the cloud provider use for encrypting data? Is unauthorized sharing of information feasible in the cloud domain? Are there any rules governing the sanctions for improper data handling by the cloud provider? Such questions, which are difficult to be answered, have made data privacy one of the key obstacles to the expansion of cloud computing.

In order to establish an assurance mechanism that will provide users a level of confidence in using a multi-tenancy cloud service, cloud service providers will need to have a focus on the inherent issues with multi-tenant architecture. Methods such as using heterogeneous RDBMS or NoSQL systems can be used. Using its own physical computing resources is another possible method, although such an approach would sacrifice the advantages of cloud computing. However, insurance companies that are concerned with data isolation need to take some time evaluating a potential cloud provider's solutions. Proper solutions can provide the level of confidence that will allow insurance cloud applications to be developed, and customers can also be assured that their data will be handled properly, utilizing the economies of scale that cloud computing can provide.

4.2. Access Control Mechanisms

Cloud-based multi-tenant infrastructures are often viewed as a cost-reducing category in outsourcing, but it is not as easy as that. It requires clearly defined terms on what services to perform, how to perform them, and what are the limits of resources and possibilities. There is also a considerable risk of what if things go awry? Who is liable for any breach of the information? What information is critically sensitive? Is it insurance policies? Is it financial information? Is it personally identifiable information? What risk is each party willing to undertake, and are those risks acceptable? What remedies are in place should something go wrong? After all this fact-finding mission has occurred, laws and regulations may come into play, such as various data protection regulations and any other pertaining to any of the tenant organization operations. All these guidelines may add up to a compilation of guidelines that may become the facto recipe when architects use access control and authentication mechanisms.

Authentication and access control inside cloud environments add security layers to address these issues: User authentication schemes make sure that a user is who he/she claims to be and that the proper controls are in place. After authentication, strong access controls are needed to enforce separability of data for private clouds, and privacy mechanisms for public clouds, ensuring that entities can only access and share the resources permitted by the provider. Authorization policies are needed to provide users the information-sharing rights they deserve. For multi-tenant systems, software must be built with

nested access control, or hierarchical views of the data. Lastly, accounting is essential. Infrastructures need a way to provide regular reports both on who accessed what information and what they did with it. This last expert audit report should hold in case any party wishes to tax the cloud operator.

4.3. Compliance and Regulatory Issues

There are significant compliance and regulatory challenges that accompany operating insurance applications in the cloud. The primary challenge regarding compliance is meeting regulations that address the security of sensitive data at rest and when being processed over the wire. Some controls that are extremely difficult to comply with are especially important in a representative sample of an insurance operation where both credit card authenticated and non-authenticated sessions are typically operational. A common security control recommended for credit card number processing is to create a separate instance of the application, a sandboxed environment disconnected from the Internet, to be used for the creation of the payment form, called the compliant payment page.

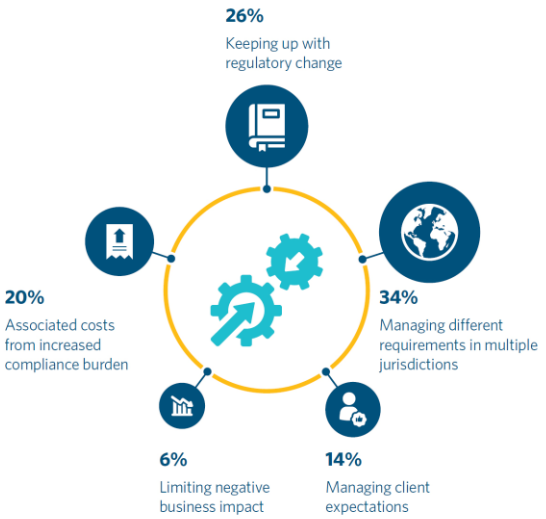

Fig 3 : Regulatory compliance

This is not feasible for multi-tenant insurance operations. Third-party tools providing as a service to evaluate compliance of cloud infrastructure may not be able to validate compliance or certificate expiration status of backend services and APIs. The problem magnifies greatly for the insurance operation who has to leverage multiple third-party services hosted in the cloud. Consumer and patient protection laws contain provisions about the security of sensitive data, but also regulations in terms of which third parties can handle sensitive consumer data. Depending on the financial instruments being adopted, the insurance operation is likely to be governed by new government oversight entities who may impose additional consumer protection requirements around things like updates to smart home devices, notice of failed remote entry features, or cybersecurity training for home warranty insurance agents.

4.4. Threat Landscape and Vulnerabilities

The increasing prevalence of multi-tenant cloud architecture raises a series of new security issues for all tenants and the service provider as well. All tenants' computing resources are directly provided by the service provider and are optimized to share resources to enable mass business reduction costs. In this architectural model, all tenants deploy their applications into the same cloud service data centers. Therefore, the best mechanism to avoid cross-tenant data access is to use the role-based access control mechanism. Many universities and educational institutes use a cloud-based learning system with multi-tenant architecture. They have many different data modules to examine students' exam records for easy data access at any time. The service provider needs to aggregate all tenants' data for more reliable well-accepted services.

However, some services cannot help but store tenants' confidential data. Therefore, the provider must protect it carefully for integrity data protection, to protect it against being deleted or manipulated by unauthorized access to be trustworthy. However, in our model, both the service provider and users can use their own separated keys to encrypt their mapping tables and files to prevent unauthorized access. A multi-tenant model adopts a system structure that was previously

used by a cloud service provider. In addition, inside the service, an internal security mechanism or security protocols that the service can adopt need to be put in place to enhance all tenants' data protection. Vulnerabilities can allow an attacker access to exploit access to the data the architecture hosts. Therefore, all tenants need to establish certain policies against those implementation vulnerabilities.

5. Impact of Cloud Security on Business Operations

Cloud computing is central to nearly all technology-related business decisions today. Why would any organization deploy a business process in the data center it owns, operates, and manages when they can reap significant savings by deploying it in the Cloud? Cloud Security has emerged as one of the foremost inhibitors of business process expansion into the Cloud. Every organization is careful to choose the right cloud provider and determine the right cloud deployment model. Security has emerged to be the pivotal factor that constrains the scope of movement into the cloud. Security has been questioned in almost every single deal where the Cloud provider has offered significantly lower costs and considerable efficiencies when compared to operating it in-house. Security in the Cloud has become a serious discussion topic that has often gained much higher priority than scalability, efficiency, or pricing. More importantly, security has become the deal breaker that has forced Cloud providers to rethink their security architecture. Cloud Security is no longer a question limited to the IT security team. It is a question that gets asked by the Board of Directors and the CEOs of organizations across every industry and geography.

In fact, the first step any organization wanting to become a Cloud service provider would take is the implementation of a strong Internal Control mechanism to ensure that their data, computers, systems, and employees are protected against security breaches. A document describing the Internal Control Policies should be created in consultation with a networking expert to cover and enforce all the major tenets of managing internal security. These tenets must include porous zones that don't require password protection, a Private Network that verifies user identity to control entry into sensitive systems, a Cyber Fence to detect break-in activity, use of passwords, personal identification numbers, smart cards to restrict access into private systems, established rules for standard use of computing and networked systems, prohibitions against insider abuse, a policy on employee use of the internet and Email, and policies regarding data backup and storage and monitoring of systems to detect and investigate security breaches.

5.1. Operational Efficiency

Increasingly, IT departments are expected to supply cloud security protection quickly as business units launch cross-tenancy initiatives with partners and third-party vendors to build the latest apps, which these internal users can deploy without security consent. This demand exists, even as security teams request more time to process data-sharing requests, audit new systems, and do risk assessments on their customers and partners. The status quo of putting apps in different silos to separate tenants is not enough, given the need for companies to offer intelligent viewpoints—like risk scoring—that mesh access to multiple tenants with machine learning algorithms and massive datasets in the cloud. The need for operational efficiency demands a better, more agile way for a security team to build protections around Multi-Tenancy applications that make cross-tenant initiatives possible. Triage where something is homegrown or enterprise grade is a key part of building a cross-protection architecture like this. A cloud security workload can be built that will handle the vast majority of commercial off-the-shelf packages. Large COTS SaaS packages are increasingly built out of cloud-native tooling, such as authorization frameworks, serverless functions, and other cloud-native services. In some ways, enterprise-grade multi-tenancy security is just the

first tier of what those products protect across all their customer organizations—called commercial off-the-shelf SaaS in security jargon. You can think of COTS packages as boundaryless systems with deep connections for providing go-hosted business logic. However, large enterprises generally cannot use these services without delving into their settings to customize how deep those hooks are—not unlike the path an enterprise SSO solution typically takes to fully integrate with an IAM system.

5.2. Cost Implications

Cloud technology, when applied to our current organizational model, propels many business processes to run faster and cheaper. Whenever an organization embraces cloud service, especially public cloud model, they save interim costs. The CSU model provides several patterns to run insurance operations faster and cheaper while changing the operational model. The value of reducing these operational costs impacts the cornerstones for pension calculation, customer applications, and agent incentives.

Any business transformation project lays heavy concern on its cost implications. Most of the project's results will impact their business outcome. Under the proper cloud security guidelines, our organizations may minimize the cost implications. Public clouds offer a new way for businesses to provision and pay for IT services. Business process and technology are becoming a commodity. What is needed is a way to assure companies their information is secured while being stored managed and used by the service provider.

One of the biggest hurdles for SOA is the overnight cost implications. No company can tolerate a one-time investment of hundreds of million dollars for software application changes. Companies must find a way to experiment with creating network change and design policy to test the new processes without major interruptions or currency implications. The way to enable lower-cost entry is by using the cloud environment. Once the concept is proven in the cloud, the financial and technical models can be worked out for implementation on the organizational SOA services.

5.3. Customer Trust and Satisfaction

Securing sensitive data while enabling smooth and seamless business operations is a tough balancing act for insurance providers that are migrating from traditional on-premises infrastructure to modern multi-tenant cloud architectures. Even the best-laid migration strategies can run into complications, and bad experiences will likely linger in clients' minds, resulting in further hindrances to overall customer trust and satisfaction. Slow and sparse responses to client inquiries can frustrate customers, especially when they are in times of need. Any downtime or lost functionality also seriously undercut the credibility of the insurance provider and damage the positive perception that clients have developed toward the organization. Data leaks that expose highly sensitive information about clients can irreparably devastate this prior goodwill and potentially lead to customer abandonment. Customers may not be aware of the key advantages that cloud security solutions offer in terms of flexibility, scalability, and availability. Yet they will blame the insurance company for any interruption or delay that occurs in the transaction process at their end. The case is made even worse when companies either do not communicate openly about downtime or data losses or do not manage these negative incidents well. Simply acknowledging the difficulty and apologizing does not assuage the damage—honoring potential compensation as goodwill has to be a consideration when trying to make customers happy again. If the compromise affects critical business operations from the client’s perspective, such as filing claims and accessing the insurer's data, no amount of apologies or discounts would work in mending the relationship. Insurers have to act promptly, coming up with workable plans that address the issues, restore service, and uncover what went wrong in the first place.

6. Best Practices for Securing Multi-Tenant Architectures

Multi-tenant architectures are being used for deployment of insurance enterprise solutions built on modern technologies to reduce deployment time, maintenance costs, and to improve scalability. These type of solutions are highly attractive as compared to legacy solutions because of hardware equipment consolidation, shared platforms, and centralized service delivery that reduces operations costs. However to reap these benefits, organizations should pay careful consideration to security if these solutions are to be deployed within insurance organizations which mainly handle sensitive personal data. While service providers of multi-tenant architectures maintain security measures at the datacenter and networking levels, the organizations deploying the applications should take the responsibility for protecting their applications and data.

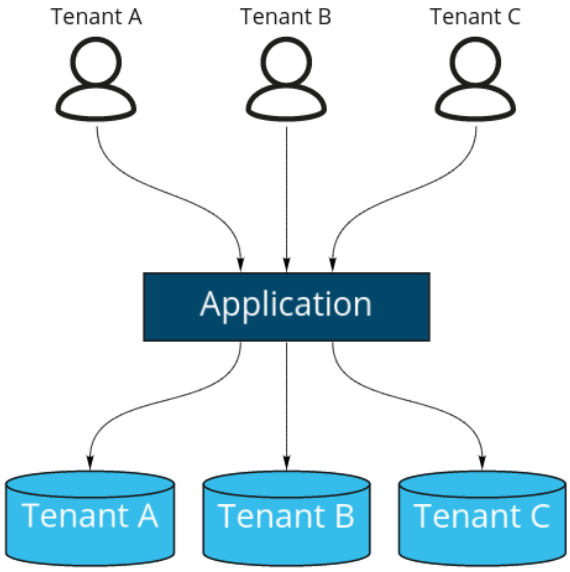

Fig 4 : multi-tenant in computing

Organizations that deploy enterprise applications on multi-tenant environments have to think about security configurations carefully and stay vigilant. A well-defined governance framework and security operations policies with specific tools and automated processes to close gaps and mitigate potential risks and threats will help decision makers to implement and continuously improve a robust security and compliance strategy. This section describes best practices to enhance security of enterprise applications deployed on cloud infrastructure managed with multi-tenancy architecture.

6.1. Implementing Strong Access Controls

Enterprises are concerned about unauthenticated access by cybercriminals scanning for vulnerabilities, as well as misconfigured authentication settings or when user accounts are compromised. In fact, cybercriminals can use a compromised identity to gain access to sensitive and privileged resources. Multi-tenant architectures can increase the risk associated with identities in the cloud as they allow the potential of acquiring identity privileges with access to multiple tenants. In addition, multi-tenant architectures that support marketing also expose users to greater risks while utilizing face biometrics identifiers. As a result of this concern, many people have instituted bans on identity checks conducted while users utilize face biometric identifiers. However, it is difficult to secure network-accessible devices from identity-related risks. As a result, identity risks have become a persistent concern for organizations digitizing their business using cloud services.

Fig 5 : PCI DSS compliance best practices

With the increased concern about identity-based risks, people and organizations are concerned about stolen credentials, access to cloud environments without multi-factor authentication, and user impersonation catering to sensitive information. In cloud multi-tenant environments, there are various

scenarios for identity risks to arise. Various scenarios for identity risk in multi-tenant cloud environments include stolen credentials for public-facing resources, absence of user impersonation controls for data storage, and lack of multi-factor authentication within the identity lifecycle. Implementing strong access controls is imperative in mitigating the risks associated with users. By instituting strict access controls, organizations prevent unauthorized users from gaining access to sensitive systems and help mitigate data loss, damage to the infrastructure, and financial fraud.

6.2. Data Encryption Strategies

Our reliance on cloud-based applications exposes inherent and unavoidable on-going risks from attackers. As these applications are hosted on shared infrastructures with shared data repositories, it becomes critical to understand how these architectures ensure that a customer can only access their own protected data, and not that of other customers. Multi-tenant architectures are particularly vulnerable to protectable violations of proprietary client-specific data or inadvertent unauthorized access or exposure to this data. While these risks can never be completely negated, there are certainly steps and policies that can be put in place to mitigate the risks by applying strong security policies and practices, performing regular security audits, and enforcing strict access controls. Simply relying on strong access control techniques is simply not enough to mitigate the risk inherent in multi-tenant architectures. Encryption of data at rest, in transit, and in processing have become essential best practice security policies. Of these, encrypting data at rest is usually the least complex step. Doing so will ensure that attackers who compromise the accessibility and integrity of the common data repository will not have access to usable data. In worst case scenarios, however, cloud service providers may still have access to the unencrypted plaintext data at any point in time. This may expose the multi-tenant cloud infrastructures to risk from rogue employees, or legal actions. Under these two scenarios, the stored plaintext data may still be accessed, accessible to third party companies. While such actions might be serious breaches of agreements between customers and providers, and tricky legal situations, contracts alone may not prevent customers from misusing data if permissible under law.

6.3. Regular Security Audits and Compliance Checks

Regular security audits inside insurance companies' multi-tenant IT environments are an absolute necessity to ensure that security measures are effective, data is protected, and compliance policies are being strictly followed. Compliance gaps in laws, regulations, and industry standards can expose companies to reputation and potentially very costly data loss incidents. Furthermore, many compliance stakeholders are demanding transparency and seeking continuous compliance, rather than simply proof of compliance at the end of an audit cycle. This demand for increased transparency and assurance of compliance with laws, regulations, and standards can shift the compliance landscape to a focus on continuous monitoring.

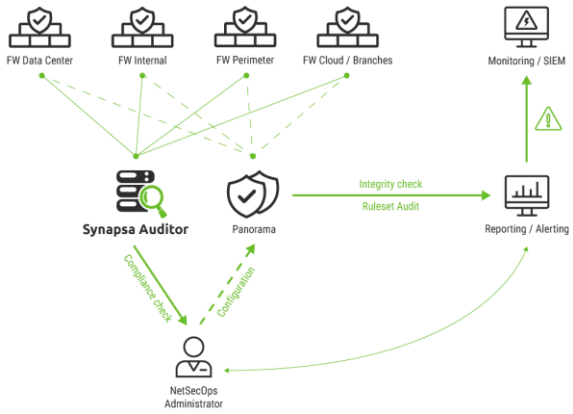

Fig : Synapsa Auditor | Compliance

Continuous monitoring helps to considerably strengthen the controls and auditing framework. Monitoring can also avert noncompliance in real-time and alert the security teams to take remedial action. In addition to internal security controls, insurance companies also need to rely on the cloud provider's security services and monitoring. Internal

and external audit teams should perform regular assessments, conduct risk assessments for business-critical processes, and map layers of the tenable advisory framework to the enterprise architecture. They should also assess the cloud provider's compliance posture, certification capabilities, and audit plans around annual operations.

Compliance and security controls must be automated in cloud infrastructure to minimize human error and maximize efficiency. Automated tools are available that can check any of the security controls listed, report on their results, automate deployment, or help to manage and report on exceptions. These tools can further be integrated into flows, making the governance both automated and proactive. Automated controls are especially useful for companies who are new to the cloud or utilizing heavy workloads in the cloud as methodologies are utilized. Scale operations and the need to deliver products quickly increase the need for automation. Solutions from providers can help companies achieve their compliance goals.

6.4. Incident Response Planning

Industry best practices recommend hosting and servicing mission-critical insurance operations and data either in self-hosted, private cloud environments or by dedicated with no other customers sharing cloud infrastructure. In the event of hosting multi-tenant services in a public cloud environment, a business' incident response plans for security events and incidents must be tailored for the unique architecture. In particular, with public cloud-hosted multi-tenant architectures, it is important to participate, agree with allocation of roles, communications paths, plans of action, and allocate critical decision-making for handling incidents in a shared responsibility model. Depending on the incident, there may be more than one responsible party who need to work together or elements may be at cross purposes and create further loss. Roles define the reporting structure and accountability to affected customers. Depending on the specifics, it may be necessary to notify other customers of the host services when shared resources or dependencies are affected, or the investigation and mitigation may impact their operations as well.

Eqn 1 : Incident Response Readiness Equation

$$\text{Response Effectiveness} = (D + P + T + C + R) \times E$$

Where:

- D = **Detection Capabilities** (real-time monitoring, threat intelligence)
- P = **Preparedness** (documented plans, playbooks, defined roles)
- T = **Team Training** (incident response drills, tabletop exercises, skills readiness)
- C = **Communication Protocols** (internal and external escalation procedures)
- R = **Recovery Processes** (system restoration, data integrity, business continuity)
- E = **Execution Speed & Coordination** (how quickly and cohesively the plan is activated)

Estate internal penetration testing against multi-tenant architectures should specifically explore scenarios of incidents that might occur and validate the role allocation and incident response plans. These should be included in the plans for forensics and re-segmentation after a successful or attempted incident is validated. Specific areas of focus should be applicable for all agreed on participant roles in a shared responsibility model, notifications of affected parties, reporting of incident impact to affected parties, and communication of decision-making processes and timelines. Special consideration should be provided for incidents involving hosted communication, notification, documentation, or monitoring for physical-world decision-making, authentication, operations of companies within critical infrastructure sectors, and management of life-saving and life-safety affairs in vulnerable populations.

7. Case Studies in Insurance Cloud Security

Modernization while ensuring security has made the insurance industry's journey into the cloud very complex. There have been several attempts to both successfully and unsuccessfully modernize insurance operations on the cloud. We provide both a critical analysis so that security does not become a final afterthought in the multi-tenant architecture employed by insurance companies both in consumerization efforts for administrative processes, as well as in consumer-facing efforts to improve operational efficiency and user experience.

In a simple test to show the weaknesses inherent in older models of deployment, a security expert created a mock up of an application built on a common or shared cloud server. The case study demonstrated the ease in hacking into personal data that was traversing the common server from multiple health institutions. Each healthcare establishment had its own cache of data on patients utilizing the shared server. The data held by each healthcare establishment was not the same across the cache in the common server, so when the different data packets traversed the server, it was easy to ensure that relevant patient data from the other healthcare establishments were hidden, while accessing the one housing the data of interest. This mock-up demonstrated the need for better security solutions over a simple deployment on a shared model of cloud architecture. Encryption was the solution for these types of attacks

Eqn 2 : Insurance Cloud Security Success Equation

$$\text{Success} = (SC + DP + CA + CM + IR) \times OE$$

Where:

- SC = **Security Controls** (identity management, encryption, firewalls, zero trust)
- DP = **Data Protection** (data classification, backup, DLP, privacy enforcement)
- CA = **Compliance Alignment** (adherence to regulations like GDPR, HIPAA, NAIC)
- CM = **Continuous Monitoring** (SIEM, real-time alerts, anomaly detection)
- IR = **Incident Response Preparedness** (response plans, drills, automated recovery)
- OE = **Operational Execution** (implementation quality, staff expertise, vendor coordination)

Several other case studies point directly at the need to have a stringent protocol and regulatory compliance when moving critical medical and business insurance data to any cloud model of storage. In the rush to adopt the cloud, many businesses depended heavily on their cloud service providers. It was noted that it was the insurance business' responsibility to use a proper data classification process and determine what to keep in the cloud. They should know the operations scope and security technology used by the cloud service provider and how this is implemented.

7.1. Success Stories

The contributions to many chapters in this book lead to the conclusion that the value proposition for cloud adoption in insurance is driven by efficiencies in normal business processes, often delivered through APIs. Indeed, we have identified a number of successful cloud service implementations in insurance; the highlights of those implementations are listed in tables, with a description in sections. Other contributors have pointed out that cloud service offerings in the insurance space are being rapidly developed by technology companies. One table shows how those technology partners can offload selected components of disruptive change to a trusted third party. We have focused mainly on non-core business functions for transition to the cloud, which are primarily business services processing massive transaction volumes where pay-per-use pricing models apply. The implementation partners have used SOA and APIs to allow insurance companies to implement those non-core business functions in partnership with cloud service vendors, with the necessary safeguards in place to protect confidential customer information. We categorize them as SaaS where end users interact with it through a web interface, or BSaaS where customizable business functions are exposed through an API for integration with insurer workflows. Examples include policy processing, claims administrative function, document management such as storage and retrieval, electronic communications including an agent portal, risk analytics, payment processing, even predictive analytics such as cat models.

7.2. Lessons Learned from Failures

Countless organizations adopt cloud technologies, but few have long-term trust-based relationships built on successful transformation. Clouds seem magic: move data to the cloud, obtain inexpensive services, and gain immediate scalability without a costly hardware purchase. Enthralled CTOs sometimes rush to the cloud without realizing the limitations it introduces on transformation. They sometimes forget that while multi-tenant

architectures may provide low-cost solution options, that behavior penalizes the organization for the failure of others. Insufficient attention to cloud security can jeopardize the very existence of a classic EA, and of the transformation itself.

The true lessons learned from that experience exemplify the risk of adopting cloud providers who ignore security standards. The pressure from employee travel schedules almost caused a catastrophic mistake when the vendor was attempting to set up a software sandbox environment. Ignoring cyber risk and finance security measures, that vendor attempted to connect to the company's corporate network using a service that prevailed at one of the travel-laden employees in a hurry. Had the employee chosen to ignore the travel and done an appropriate security assessment based on the corporation's risk standards while still working from a plane, they would have detected that the service failed to meet the corporation's requirements. They had to scramble to remove the account from the service, preventing a serious and expensive breach.

Enterprises should safeguard the first premises accessible from the outside world while relying on cloud solutions as resources increase to address digital navigation strategies. Cyber risk theories may determine how well or poorly those precautions must fare. The insurance enterprise itself must heed those guidelines in selecting which department policies may allow less stringent security provisions with general security provisions. Otherwise, the initial methods for dismissal from consideration of that policy must return to a manual process, even if complicated by years of declining establishment deterrent value.

8. Future Directions in Cloud Security for Insurance

As we reflect upon the future of cloud security for insurance and other enterprises that are being increasingly changing to leverage hybrid and multi-tenant architectures, we first need to identify some of the emerging technologies which will give a shape to the services offered by new security paradigms. Some of these emerging security technologies include post-quantum cryptography, blockchain, Zero Trust Protection Model, Self-Healing Systems and Adaptive Security Architecture. Post-quantum cryptography aims to design a public key infrastructure that secures against quantum computers and that further aims to help investment and development of post-quantum systems by academic and industry partners. In industry, our primary sources for protection are the large projection companies in the latter area including services. Blockchain technology enables always-on systems and provides opportunities for always traceable transactions. Industries of a multi-tenant texture can leverage blockchain to manage service levels and enable auditing permitted data operations without the delays of having to call in these decisions to the service owner for verification.

Eqn 3 : Future Cloud Security Maturity Equation (Insurance

$$\text{Future Security Maturity} = (ZT + AI + DP + CA + AE) \times AF$$

Where:

- ZT = **Zero Trust Architecture** (identity-first access, micro-segmentation, continuous validation)
- AI = **AI-Powered Threat Detection** (machine learning, behavioral analytics, automated alerts)
- DP = **Data Privacy & Sovereignty** (geo-compliance, encryption, privacy-by-design)
- CA = **Cloud-native Automation** (auto-scaling security, DevSecOps pipelines, policy-as-code)
- AE = **Advanced Encryption & Confidential Computing** (homomorphic encryption, secure enclaves)
- AF = **Agility & Flexibility** (ability to rapidly adopt and adapt to new technologies and threats)

In addition to these security approaches are those empowerment functions across enterprise equipment operations in a given multitenant architecture so that these systems are providing adaptive protection and predictive capabilities when faced with system storms of possible and approved attacks against the core systems. Central to the success of these solutions is predictive analytics through embracing the full bloom of Artificial Intelligence. These include utilizing recent re-architecting of clouds around containers and orchestration technologies combined with message queue processing with parallelism enabled from using the cloud's processor and resource service utilization enabling co-management of message integrity and expediting time delays across tenants

through being able to manage message rejection and trials through a parallel infrastructure resource.

8.1. Emerging Technologies

Within the insurance domain, securing sensitive consumer data and applications is critical for enabling and supporting an efficient customer experience. Data privacy and cybersecurity are paramount as consumers increasingly adopt digital methods of conducting their insurance business from their home devices, while cybercriminals continue with existing tactics such as data breaches and phishing campaigns and create new ones. Much of the contemporary technology-related literature addressing insurance consumer facets of cloud security focuses on either service provider or business factors, such as trust, compliance, transparency, accountability, and partnerships. In addressing the security of cloud computing technologies used to enhance the consumer experience, we focus on two areas.

Other emerging technologies that providers are adopting to enable and enhance digital transformation and modernization include microservices, containers, serverless computing, and blockchain, which share and can leverage the cloud technologies mentioned in the preceding paragraph. The microservices and containers, as well as serverless architectures extract much of their efficiency and synergy from shared resources enabled by commercial clouds, both hybrid and full public. Security experts agree that utilizing such architectures creates risks for the insurance enterprise and its consumers that providers must mitigate through extra security measures. For example, the application security needs of microservices and container architectures are specifically mentioned in recent discussions on the current state of cloud security. The mitigation priorities of new and unique security challenges to application security posed by microservices and containers is an open research question in the cloud security literature.

8.2. Predictive Analytics and AI

Artificial intelligence (AI) and machine learning (ML) are some of the most disruptive technologies changing the insurance industry. They have the potential to drive dramatic reductions in damage and loss through the automation of the major parts of the process. They are being increasingly acknowledged by technology companies who have developed them, as well as academia; with organizations that offer data science credentials, with job markets that have seen a substantial increase in interest. Specialized technology firms for insurance companies have generally jumped on the bandwagon with a mix of niche solutions for the insurance industry, either AI or ML-driven.

AI uses predictive analytics by substituting intuition-based human decision-making processes. Predictive analytics can detect complex hidden patterns in vast amounts of data. Artificial Intelligence enables differentiating not only business transformation but many transactions fundamental to a business. AI facilitates rebuilding and refocusing business ideas from core origin and attaching them to transformation; they allowing both prediction of risk, pricing of simultaneous products and services, underwriting for cyber risk, and modeling creation/transformation; other than checking demand-side transaction behaviors on the other side, while transformation can also foresee demand-side market behavior changes. Increasingly, reinsurers are offering insurance companies the market tools to collect and pre-process data efficiently and where predictive driven AI algorithms automatically churn the information to gain business decisions, equipped with high-speed servers where fluid data storage is architected.

9. Conclusion

Modernization of traditional insurance operations through cloud computing has been gaining traction over the last several years. The pandemic underscored the importance of cloud computing for a new-age embedded insurance ecosystem that

requires embedded insurance in a predominantly self-service mode. During this time, insurance companies emphasized expanding their digital-first engagement with customers and considering the importance of a multi-cloud, multi-tenant architecture that encourages innovation in new-age embedded insurance. However, transition from traditional IT infrastructure of on-premises data centers implementing monolithic applications to a modern cloud architecture using cloud-native applications based on microservices is a challenging yet essential endeavor.

In this essay we lay out the basis of multi-tenant architecture for a cloud-native, consumer-centric, modular insurance ecosystem that supports embedded insurance. We highlight the importance of solving the cloud security challenges during transition to this architecture. Further, we also discuss the critical next steps that would assist insurance companies in plugging the security holes in the currently views, creating awareness for potential cloud security incidents in innovation, and identifying and institutionalizing potential incentives to performers of security functions in order to develop trust in the cloud ecosystem. Current client and insurance vendor trust in a traditional shared services architecture is extremely weak, and creating trust in a cloud-native multi-tenant architecture is likely an even more daunting venture. However, without solving the issue of trust, we risk missing the innovation of exciting new-age embedded insurance products on a modern cloud infrastructure.

References:

1. Serón, M., Martín, Á., & Vélez, G. (2019). Life cycle management of automotive data functions in MEC infrastructures. *arXiv*. https://arxiv.org/abs/2303.05960
2. Pillmann, J., Wietfeld, C., Zarcula, A., Raugust, T., & Calvo Alonso, D. (2018). Novel Common Vehicle Information Model (CVIM) for Future Automotive Vehicle Big Data Marketplaces. *arXiv*. https://arxiv.org/abs/1802.09353
3. Berezovsky, A., El-khoury, J., Kacimi, O., & Loiret, F. (2018). Improving lifecycle query in integrated toolchains using linked data and MQTT-based data warehousing. *arXiv*. https://arxiv.org/abs/1803.03525
4. Capgemini. (2018). Premium OEM leverages IoT-based data in the Cloud to track vehicles in distribution. *Capgemini*. https://www.capgemini.com/news/client-stories/premium-oem-leverages-iot-based-data-in-the-cloud-to-track-vehicles-in-distribution/
5. Shiklo, B. (2017). IoT in the Automotive Industry: Concept, Benefits, and Use Cases. *ScienceSoft*. https://www.scnsoft.com/blog/iot-in-automotive-industry