IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

Implementing Scalable Identity and Access Management Frameworks in Digital Insurance Platforms

Balaji Adusupalli[1], Sneha Singireddy[2], Lahari Pandiri[3]

DevOps architect - Small commercial Insurance, Balaje.adusupalli.devsecops@gmail.com,

ORCID: 0009-0000-9127-9040[1]

Software Engineer, snehasingreddy@gmail.com, ORCID ID: 0009-0009-8450-5404[2]

SR Systems Test Engineer, lahripandiri@gmail.com, ORCID ID : 0009-0001-6339-4997[3]

Abstract: Digital insurance services already provide consumers many benefits; however, they bring multiple risks as well. Privacy and personal data protection risks, attacks to the cybersecurity model, fraud, misinformation, among others, threaten these consumer benefits in a direct way. The growing challenge for policy makers is to guarantee data protection and control for consumers while not undermining the role of other stakeholders such as capital markets and financial institutions. Although the limited time frame for the implementation of the relevant regulations is a huge challenge for the relevant authorities, it should not lead to generic solutions, which without knowledge of the specific context and of the opposing stakeholder interests will not work appropriately. Moreover, they should not lead to models which cannot be implemented easily and quickly in practice. The design of transparent and resilient digital identification frameworks should take place after careful examination of the public and private ecosystems and of their intrinsic characteristics, in close cooperation with societal stakeholders, and focusing on proper incentive schemes.

Insurance companies introduced improved scalability and resilience in their digital identity protection approaches, but at the resulting higher costs. The policy makers now face the challenge to improve the protection of personal data and identifications on the cloud infrastructure of the insurance companies. They should remain well aware of the fact however, that quick and easy to obey regulation seems impossible. For example, decentralized identity platforms are at an early stage. Consequently, their universal implementation cannot be quick, as many stakeholders should be engaged to successfully operate through decentralized identities. On the other hand, promoting some characteristics of decentralized identity solutions through standards (or at least usable solutions with such characteristics) could be done as an initial step in a quick and effective way. Finally, understanding of context and incentives for compliance should be introduced in the design of regulations at the outset. Privacy preserving solutions that protect the consumers data and identifications are not in the best financial interests of the insurance companies as there are important sunk costs in their current digital identity and personal data protection infrastructure. Understandably, their desire for a quick windfall gain in compliance will lead to a generic regulation finally hurting consumers rights.

Keywords: Identity and Access Management; Identity and Access Governance; Digital Insurance; Cloud-based Identity and Access Management.

I. INTRODUCTION

Digital transformation is rapidly changing the modern insurance landscape. Innovative insurance products and services are introduced to the market at a blistering pace. For example, peer-to-peer insurance, liquid insurance, on-demand insurance, usage-based insurance, chat bot insurance, and so forth. Digital insurance platforms emerge to support a novel business model and innovative insurance value chain processes.

Digital insurance platforms usually integrate multiple services in one platform. The integration of 'best-in-class' services from several innovative Insurtechs into a single digital insurance platform requires a robust Identity and Access Management (IAM) framework. A good IAM framework should be able to securely manage users, roles, and digital resources. However, many digital insurance platforms face IAM challenges with the integration of third-party services. For example, how to scale the existing IAM framework to meet the demands of the growing number of integrations? How to secure the accessibility of sensitive enterprise resources for multi-tenancy environments? How to securely maintain the roles of third-party services with the growing number of changes? With these IAM challenges, the effectiveness and efficiency of digital insurance platforms may be compromised.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

To address these IAM challenges, IAM tuning proposals and IAM design patterns are extracted from the IAM literature. Based on the IAM tuning proposals, a scalable IAM framework for growing digital insurance platforms is designed. The IAM tuning proposals, the design of the IAM framework, case studies, and solution implementations are elaborated. This should provide valuable insights for digital platform developers facing IAM challenges with the integrations of multiple third-party services in fast-changing environments and for researchers seeking research opportunities on this topic.

1.1. Background and Significance

The growing demands for secure, efficient, and customer-centric services in digital insurance platforms place unprecedented strains on insurers and policyholders alike. Insurers require a sustainable approach to serve new services while improving existing offerings and capturing new customers, all while managing the complexity and capital required to support services, risk, regulation, compliance, and governance . Policyholders may find that their needs are not met adequately, leading to dissatisfaction with their insurers. Access management, comprising federated identity, single sign-on, and access policies, is foundational to successful service delivery and customer engagement. Overly complex systems can lead to user frustration, resulting in lost customers or reduced usage.

Fig 1: Identity and Access Management Frameworks.

The number, growth, fragmentation, and changing nature of customer identity and access management entities in insurance ecosystems have increased dramatically, contributing to systems becoming increasingly difficult to architect and manage. Future business models and technology stacks can be complex environments to govern and manage. Alliances of direct competitors, partnerships including internet and technology firms that potentially compete with traditional insurers, the introduction of new products by established insurers, the emergence of new providers, forcing an expansion of insurance services and the providers offering them, government regulation, and a growing array of consumer comparability and preference choice engines are all sources of complexity. Customer IAM systems are often tasked with catering to multiple products with differing, sometimes conflicting or non-standard requirements, multiplicity in the number and types of vendors, users, regulatory controls, security requirements, and convoluted orchestration logic.

Accordingly, IAM needs to expand far beyond traditional user portal systems comprising a federated identity and SSO, to address integrations with new products, giving rise to new service delivery architectures and user interactions. In parallel, the intersections between business strategy, regulatory compliance, risk mitigation, and technology infrastructure/services are increasingly complex and layered. Consequently, the foundational IAM system for a new digital insurance ecosystem can rapidly exceed existing capabilities and strategic and financial intentions. For many risk and service integrations, the user experience can be wholly new, unexpected, and difficult to deliver, and bring together the involvement of numerous technology vendors and service delivery providers.

II. UNDERSTANDING IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and Access Management (IAM) comprises the policies and technologies for managing digital identity and for controlling and monitoring the access of authenticated users to information systems. IAM strives to ensure that only the right organizations and users can access the system resources at the right time. IAM technology is typically structured into three components - management of identities, management of governance and compliance, and management of security and operations. The types of IAM solutions can be classified within an identity evolution framework that includes user provisioning, synchronization, and federation. Digital identity as a construct is still far from fully complete and standardized. A wide range of attempts to represent digital identity have been undertaken, but none have yet gained widespread uptake and use.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

Existing standards and technologies to represent and federate digital identities are diverse and fragmented. Access control is concerned with specifying and enforcement of control of access to resources. A large number of approaches and technologies for access control have been developed, and relevant works can be found throughout the literature. Beyond access control, the management of access rules and policies also comes under IAM. This component is intrinsically related to the governance of access, which in turn is tightly coupled with compliance. Both governance and compliance aspects of IAM have been recognized and the relevant challenges better defined in the past couple of years.

An IAM framework was proposed along with brief overviews of IAM technologies and IAM challenges. To derive an IAM framework, the most relevant IAM circles need to be extracted. Standard IAM frameworks contain components to manage identities, access control, governance and compliance, monitoring and auditing, and security and operations. IAM technology platforms have compliance requirements in particular for industries who make large use of e-business gateway solutions. First drafts for IAM frameworks can be found in the literature, but these were treated as vendor specific descriptions with little analytical grounding. IAM components can also serve to describe existing IAM implementations and to assess strategic decisions concerning IAM technology implementations.

2.1. Definition and Importance of IAM

In today's interconnected world, individuals, businesses, and devices all have a unique identity. Digital identities have become a leading “resource” to be exploited, and companies have gathered a wealth of information about their users. Realizing the potential power of this resource, service providers coerce users to create and manage digital identities. Service-related information about a user is fragmented in system-centric isolated silos. The operators of these silos exploit users’ identity data to get the most out of them. The operator’s monopoly on the user’s identity data transforms its user-friendliness into permanent surveillance, leading to the user's complete disempowerment. Resolving the resulting problems was one of the initial goals of blockchain technologies, but their immutability and other characteristics created another host of issues. With the growth of e-government, online banks, cloud services, IoT devices, etc., the number of service providers for individuals is rapidly increasing.

As a consequence, the number of personal digital identities is also increasing. Each of these diverse services requires identity-related permission requests in a completely different format. Widespread adoption and increasing maturity of the Decentralized Identifier (DID) specification promise to alleviate interoperability issues between services and approaches on how to support and exchange identity-related data. However, there should be an interoperable and extensible mechanism to register DIDs and maintain a compatible mapping with increasingly critical trust schemas. The aim is to build a community-centric privacy-enabled Decentralized Identifier and Decentralized Identifier Document storage system, a global Discovery System that is capable of performing searches and CRUD operations on DIDs without a central entity.

Governance by consensus is a common characteristic of both IPFS and blockchain networks. Several consensus protocols are being developed by the blockchain community. The best solution for the MVDDS should be an impartial, equitable, and stable consensus protocol, which should be thoroughly analyzed and selected for DVDS. These various consensus protocols must co-exist and interoperate securely and efficiently. The increasing number of nil-service authenticated DIDs disclosed by the community or a group of communities raises the need for an identity Data Bit Torrent-like file distribution/storage system capable of securely registering and granting reciprocal data access permissions on the stored data. On the other hand, access control delegation on the DID Discovery System API calls raises the need to provide service-specific, private, and self-defined access control mechanisms.

2.2. Key Components of I AM

The construction of an IAM Entity Framework including technical standards, protocols, roles, and events as a basis for flexibility of IAM frameworks and distributed implementations of IAM solutions requires the consideration of Entities. An Entity is defined as a singleton, stateless, addressed object with uniform syntax pointed to by an addressable entity. Each Entity has a type or role which provides a uniform Collection of such Entities with uniform behavior.

The Experts building the Entity Framework recommended to group IAM Entities in relevant categories. A distribution of passive Entities, which are fed with input Events and produce output Events without business logic itself, will lead to high cohesion and low coupling of IAM Entity implementations, improve scalability, maintainable, distributable and configurable implementation options. This is the basis for future work on a backend neutral IAM Representation standard to allow for the distribution of different frameworks/technologies. Additionally for future evaluation purposes it ensures the possibility to implement every IAM Agent within equal scope.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

As several communications of AQM Framework IM or AQM Cloud IM show, there are already working prototype implementations of IAM Agents providing their own IAM standards, protocols and Events. Based on the Component Structure of IAM Agents proposed in this paper, this implementation can now be expanded and simplified. It is planned to conduct a pilot study to evaluate the scalability, maintainability, etc. of such a framework-based IAM standard approach.

The definition of an IAM Entity Framework can be beneficial for others in the IAM community. It provides an approach for developers to build subsequent Entity based-assured frameworks, such as AQM standards or protocol based IAM-Agents, enabling broader interoperability comparison assessments. As a basis to contribute to the growing number of IAM standards, protocols, agents, endpoint implementations without interfering with other parties' contributions, it is of utmost importance to develop an IAM Entity Framework involving both. However, such solutions are not sustainable solutions by keeping the underlying framework proprietary if participants can only interoperate with it via its IAM Agent.

Equ 1: Authentication Success Rate (ASR).

$$\text{ASR} = \frac{A_{\text{success}}}{A_{\text{total}}} \times 100$$

- A_{success}: Number of successful user authentications
- A_{total}: Total authentication attempts
- Measures the system's reliability in handling user logins, including scalability and access responsiveness.

III. DIGITAL INSURANCE PLATFORMS OVERVIEW

Digital transformation has driven organizations to adapt their operational processes through advanced digital solutions. This shift has influenced all sectors, including insurance services, which are gradually transformed digitally with the rise of digital insurance platforms. Along with the success of the insurance digital transformation and the evolving digital insurance platforms, growing concerns arise.

On the bright side, digital insurance platforms enhance consumers' insurance product autotyping efficiency, broadening access to insurance and lowering premiums. However, the insurance digital transformation challenges traditional insurance models and faces innovation barriers in terms of knowledge co-creation mechanisms and service ecosystems.

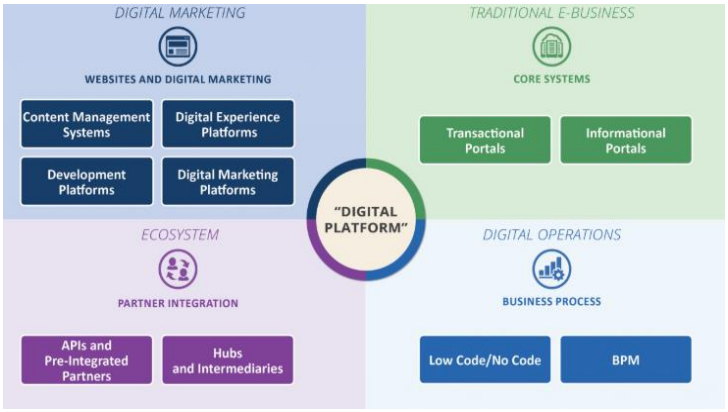

Fig 2: Digital Platforms in Insurance.

Digital insurance platforms are cloud-based, multi-sided platforms through which completing disruptive insurance industry transformations economically, technologically, and socially. A three-dimensional digital insurance platform taxonomy is introduced, assisting practitioners and researchers in better understanding digital transformation processes' traits, including architecture, governance mechanism, and value proposition. Existing taxonomies use abstract dimensions, while the other taxonomies get overly granular.

Notably, information asymmetry between insurers and insured impedes efficient risk pricing and management. The two parties are separated through digital insurance platforms, hindering cooperation and collaborative risk management. Insurers attempt to embrace digital insurance platforms, establishing a direct trilemma among data ownership, capture, and control, which must be resolved.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

3.1. Current Trends in Digital Insurance

With a medium score of 67%, the Long Pools, Weather Index Insurance, and Weather Risk Transfer are among the current trends in digital insurance. It ranks above average and ahead of Property Damage by 11%. Nonetheless, it is ranked below Liability Insurance and the Emerging Market. Despite variables such as COVID-19 pandemic data that affected the world throughout 2020, the implementation of the weather index insurance in more emerging countries was lower. Nevertheless, index insurance is a promising product for agriculture and SMEs, which constitutes a considerable proportion of business opportunities. As a consequence of natural disasters, goods transported by road, air, sea, or railway may be lost, stolen, or misrouted. In addition to that, cargo insurers typically have disputes with handle counterclaims for loss to valuable goods in transit. The insurance index is digitally analyzed through AI algorithms and blockchain, and if the index differences surpass the preset value, the insured will receive immediate compensation without additional paperwork. As the average person possesses seven connected devices, an insurance premium can be set based on these devices and how the data is utilized. Compounding the effect of adopting various schemes of connected gadgets, if only one of them is not properly used, the device being adopted is charged a high premium.

The majority of consumers 65% of millennials are willing to share personal data with insurers in exchange for reduced premiums; insurers can enhance conversion rates by 25%. Utilization of a smart car and the extent of adherence to safe driving habits can be fed to underwriting bargaining. This leads to improved premium pricing, which can be verified in real-time by insurers through a chip placed on or in the vehicle. The security insurance scheme would involve tuning systems and personal data information equipment. In case sensitive data is exposed due to normal usage or computer attacks, the capability of attack origin tracking imitation incurs additional charges. For Protection for Multi-account By Attacks, questions such as which bank ATM card were toward or whereabouts when shopping will be asked to prevent multiple account theft and fines are charged for any deviation in confidence.

3.2. Challenges Faced by Digital Insurance Platforms

The complexities of modern society have created an acute need for individuals to electronically exchange authenticated and trustworthy digital identity and credentials as proof of identity in any sector. Digital Identity (DI) is important for individuals to secure access to online services such as banking, insurance, security, and healthcare. Service providers build trust for electronic service delivery based on the presented identities and attributes from the public and/or semi-public sectors. The total estimated cost of identity-related activities is a significant burden on national economies. Individuals are exposed to continuous identity fraud, stolen identity, and “identity theft” incidents. The fallout from this investment is the widespread growth of online fraud, spam, phishing, and waste of service delivery resources. Consequently, cardiovascular data on banks cooperating with private parties are in danger of blackmailing.

The EU strives for a fully functional Digital Single Market that aims to foster digital innovation, create new business opportunities, and guarantee consumer protection and privacy. However, individual cross-border access to public online services in the EU is still problematic. As a result, call centers still need to handle service over a non-secure international telephone line. For service providers, providing such services entails excessive costs and risks of non-compliance with relevant regulations. Traditionally, insurance companies collect significant money and time from policyholders to examine risk. However, they stand much financial fraud occasions when inspections are based on manipulated hard copies of certificates or permits. Document-based inspections are no longer sufficient as current communication methods do not have the necessary guarantees of trustworthiness due to non-proven ownership of soft copies. New methods are needed to secure compliance verification, i.e. without exchange of provision of underlying credentials. Authentication means the act of the service user providing proof of identity to service providers. Such trust-generating attributes can be asserted in a standardized manner and use standard communication channels to be submitted, stored, and exchanged in a privacy-preserving manner.

IV. SCALABILITY IN IAM FRAMEWORKS

The scalability of IAM in digital insurance platforms refers to the ability of the IAM framework to effectively manage the identity and access needs of an organization as it grows and evolves. A scalable IAM framework is essential for digital insurance platforms because it can accommodate the addition of new users, applications, devices, and policies without degrading performance or functionality. Scalability is essential in the digital insurance sector because, as firms grow in size and complexity, their IAM framework has to cope with new challenges such as the management of digital identities, the growth in the number of clients, ever more stringent regulations, and the integration of new technologies into legacy systems.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

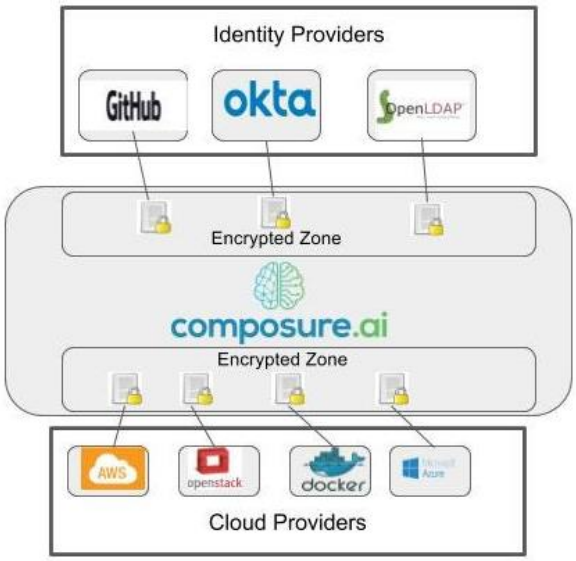

Fig 3: Scalable Multi-Cloud IAM Framework.

The principle of separation of concerns deals with the aspect of flexibility in IAM. Flexibility refers to the easy implementation of changes in the IAM framework without the necessity for reconstruction or serious modifications. In IAM, flexibility has two meanings. The first meaning involves extending the existing framework and adding functionalities without compromising previous ones. The second meaning involves the ease of changing processes supporting the IAM framework, such as the workflow rules determining how users are created. Likewise, both dimensions should be considered when selecting scalability solutions. A comprehensive IAM framework is mandatory in digital insurance to meet the requirements for digitization, to manage innovation, and to comply with regulations. Technically, the extensive use of clouds, distributed environments, and microservices must be seen and addressed.

The above-cited challenges and concepts create a complex and dynamic environment for IAM where at least three properties must be present. First, the presented IAM solutions must cope with the fast-changing environment without being reimplemented. The second property involves the transparency of IAM solutions. Frameworks must address all relevant IAM tasks and provide detailed descriptions of how these tasks are implemented on the technology side. The third characteristic relates to the adaptability of IAM frameworks.

4.1. Concept of Scalability

Scalability is defined as the ability of a system to adapt itself to changes in its load, such as the number of users, number of tasks, number of requests, and so on. A scalable system would keep its performance unaffected by such changes, or at most a little bit affected. In some cases, where such a dent in performance needs to be accounted for, the degree to which this performance drop is constant (e.g. logn or O(n)) would be defined as the degree of the scalability. Naturally, there are systems where changes in load do not at all affect performance. Therefore, perfectly scalable systems are those that keep their load undisturbed by additional load, provided that such a provision remains somewhat understandable. The demands of scalability have been taken into consideration since the inception of computing as a whole. Thus, there exist forms of scaling up where a user can submit larger requests to a batch job.

However, as the production environment gets more dynamic, with load being constantly added or removed, the need for incremental scalability and on-line approaches has been recognized as a requirement. A different alternative to metrics that measure performance on execution time is to take into account response time instead. This points out from the very beginning that scalable systems would experience no change in their performance, or, while there exists change, would have it evolve gracefully, i.e. these changes would be minor relative to the overall operations. However, scalability is also made out of categories, where the same system would be considered more scalable on some metrics and less scalable on others. Therefore, scalability is a rather subjective term that depends on loads and systems.

Scalability is defined in roughly three different enumerations. First, in a weaker, local sense, scalability is stated as existing properties of scaling in some of the above aspects, but with no bounds on the admissible sizes to scale to. In terms of a simple metric to measure, perfect scalability would mean a constant time when drawn against load size. It is trivially true that every constantly usable system is “locally scalable”.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

4.2. Benefits of Scalable IAM Solutions

The growing ubiquity of connected systems and software-as-a-service solutions within organizations increases the complexity of access management. As a result, the number of identities and access rights is inflating, leading to a steady growth of support effort without a proportional increase of business value. Here, scalable identity and access management (IAM) solutions can deliver several benefits when they have been implemented on a cloud-native IAM platform.

First, a cloud-native IAM platform provides an on-demand, resource elastic IAM infrastructure, optimizing cost and performance. With a hybrid IAM environment, an on-prem cloud-based IAM service may scale-out capacity, leading to lower ongoing operations efforts. Either scenario is economically beneficial since the utilized capacity matches the identified business needs instantly and requires no front costs. Sizing individual instances according to expected throughput allows for high starting performance while minimizing ongoing operations costs in a running system. A heterogeneous architecture can segment data to allow for extremely high performance infrastructures.

Second, minimizing the fixed support effort is a central goal of the IT department. The variable support effort is traded against a cloud-based service supply, mainly managed by the IAM service supplier. This minimizes over-provisioning of resources, leading to lower effort for regular infrastructure-related tasks and repairs, maintenance, or upgrades. Shared resources should be dynamically allocated, applying limits only on the overhead of followed properties like minimal resource spend per instance.

With a separation of concerns and agility-driven integration, an organization can reduce the ongoing cost of resource usage, regulatory compliance, cloud details, and organization changes. There shall be no dependencies on an infrastructure for any IAM service. Cloud details are abstracted by platform-perceived endpoints. Wrong IT resource choice is a strategic threat for an organization, but as IAM relies on cloud-native platforms or components, there are no dependencies on a single vendor, service, or location. Compliance is a business risk that shall not incur additional technology overhead. Regulatory compliance is guaranteed by IAM layers, and service suppliers cannot alter service security and privacy settings.

V. DESIGNING AN IAM FRAMEWORK FOR DIGITAL INSURANCE

In the digital insurance industry, Effective IAM is crucial for protecting sensitive data and managing customer information. This paper introduces an overarching IAM framework that offers a full set of IAM processes and supporting components for organizations operating social networks. The importance of reliable identity management for the trustworthiness and safety of social network systems is emphasized. While existing IDM frameworks present a set of processes and components for identity management, they do not comprehensively cover IAM for social networks. Consequently, a process model and suitable component architecture are provided for a scalable IAM framework. Additionally, two important but neglected IAM components—information auditing and credentials management—are described in detail.

A federated identity management (FIM) service model is established, detailing the benefits of FIM, its basic process, and the system components. Basic identity sniffing protocols, as well as more sophisticated federation protocols, are introduced. After analyzing sample processes and components within the FIM service model using BPMN diagrams, the paper summarizes and analyzes existing reference process models for the FIM service model. Existing federated identity models, including both widely adopted protocols and theoretical guidelines, are also presented. The above-related work on identity management is mapped back on the presented FIM service model.

Located at the top-level of the business architecture, FIM service models are concerned with high-level processes and organizational structures. Located in the application architecture, FIM system models include design artifacts that are more technical in nature. The goal of these models is to detail the components of FIM systems and their interactions within the scope of the FIM process. Relevant modeling artifacts are provided in a separate paper. Deployment models detail how applications are physically deployed and run on network nodes within the context of the business architecture and the systems being deployed. These models are represented according to the view architecture and UML.

5.1. Requirements Gathering

The requirement gathering phase concentrates on understanding and capturing the user's requirements. It creates a framework that consists of internal, external, and functional requirements. Within this phase, framework modeling addresses what the digital insurance platform must accomplish in an initial phase. Furthermore, the necessary information needed to fulfill the requirements is defined. The factors that affect the decisions regarding the modeling of the proposed digital insurance platform are clarified next. All the requirements must be gathered in a manner that allows a sequence

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

of systematic actions to validate the documentation and implementation exercise. The enacted activities include analysis of requirements identification techniques, stakeholder identification, and interacting with them to elicit requirements.

The purpose of the requirements gathering phase is to create a framework that consists of the internal, external, and the functional requirements of the proposed digital insurance platform architecture. This section has focused on the external requirements within a framework using the IFEEL technique. The required technical platform specification, constraints, human, and organizational factors to consider within the general requirements gathering phase of the proposed digital insurance platform are described as well. The external environment in which the digital insurance platform is to run has been scrutinized next. The operational and design constraints under which the proposed digital insurance platform architecture must operate are defined afterwards.

The functional requirements needed to fulfill all of the requirements gathered above are defined in the construction requirements context. The IT technical solution required to implement the proposed digital insurance platform architecture is now stated. Finally, in the Requirement gathering section of the Requirements Framework, the factors that affect the decisions regarding the modeling of the proposed digital insurance platform are clarified. All the requirements mentioned above must be gathered in a manner that allows a sequence of systematic actions to validate the documentation produced as a result of these activities as well as the eventual software implementation of the documented requirements. The enacted activities are analysis of requirements identification techniques, stakeholder identification, interacting with these stakeholders to elicit requirements.

Equ 2: Scalability Utilization Factor (SUF).

$$\text{SUF} = \frac{U_{\text{peak}}}{U_{\text{max}}} \times 100$$

- U_{peak}: Peak number of concurrent users
- U_{max}: Maximum supported user capacity
- Indicates how close the system is to its scaling limits and helps guide horizontal/vertical scaling needs.

5.2. System Architecture and Design Principles

The key design principles followed in the design of the architecture for the Identity and Access Management framework that scales into compliance with the requirements addressing the technical aspects of scalability of the Identity and Access Management framework for digital Insurance Platforms based on mitigating the risks for the business processes supported on the Platforms use cases are explained.

In general, the Identity and Access Management architecture is composed of an Identity Tier, containing Identity stores and the federated Identity management, the Regulator Tier which contains the Authorization service and the Governance Tier for governance processes from where the business complexity is managed. To ensure scalability, Data Providers expose the data to the Identity and Access Management framework to scale the Identifiers generation and enforcement. Governance processes define business processes and access rules that are made available to Regulators. The architecture illustrates the main components and the interactions between them addressing the design principles of scalability and modularity. The referred interaction is as follows.

For any Identifier that needs to be generated, an Identity Store is selected according to the types of data involved. The construction of the Identifier involves the interaction between Data Processors which generate the required pieces of information and the Data Stores where they are stored. The Identifiers are notified to the demanders. The collective Enforcement is continuously enforced by the Access Services interacting with the Data Providers, Access Procedures, Access Policy Store, and Access Rules. Then, the two components are used in the following ways. To feed data essentially by selecting the Identity Store that for the type of data, Institution, Profile, and even the Identifier. To register access essentially by selecting the Access Service and providing it with the external Identifier. To check compliance essentially by selecting the Data Provider. The data involved is also specified.

The implementation of the elements composing the architecture is now described as these implementations correspond to the implementation of the design principles defined. The fidelity of the implementation of the architecture is ensured by the following elements. A transformation layer from REST to SOAP. A custom design and Modification Access Services to ensure increased Scalability of Access Services implemented as distributed.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

VI. IMPLEMENTATION STRATEGIES

Designing a robust IAM infrastructure involves several activities, including analyzing and documenting business applications, architecting the IAM framework, implementing/re-implementing IAM components, migrating existing applications to the new framework, and deploying the new infrastructure. Getting the first few applications right is critical to success. Given the commercial and reputational risk, priority is placed on getting it right first time. Mistakes or issues made on the first few applications will generate disproportionate amounts of political and commercial fallout.

Users with business critical accounts must have their credentials migrated to the new IAM framework. These accounts generally must have been used within a month of the migration. It's also useful if the user has performed a high-risk transaction recently. Once users submit their credentials, then (given a successful migration) access to those applications is enabled immediately.

Any user accounts being migrated to the new IAM framework that haven't been used recently cannot have their credentials migrated as above. Accordingly, these accounts are locked prior to the migration. A standard notification mechanism will be triggered to inform users of the lock, including necessary steps for re-enabling access. Usually, if applications are migrated either side of an account lock, criteria that normally allow the user to reset their password must be met. Generally, as account lock notifications on the previous account may have been missed, an email and SMS notification will also be sent to advise of the lock. Additionally, appropriate controls on newly registered accounts are required. These would generally continue for at least a period until users were sufficiently familiar with the new mechanisms. Account migration should also be audited. Reports indicating which critical users had their accounts migrated, locked and/or failed will assist compliance.

6.1. Agile Methodologies in IAM Implementation

Identity and Access Management (IAM) is an essential part of each organization's infrastructure. Replacing existing IAM tools with a cloud-based platform providing out-of-the-box IAM capabilities is challenging. Acceleration of the adoption process requires restructuring the existing way of working and introducing new methodologies. This case study presents a way for IAM to adopt DevOps principles, practices, and tools to speed up the processes constantly demanded from IAM teams and to be able to handle them without a need for additional headcount.

Many organizations rely on existing tools to deliver a lot of identity-related functionality. These tools require considerable effort to maintain and do not meet the market demands for innovation. Replacing existing IAM tools with a cloud-based platform that provides out-of-the-box IAM capabilities limitations as well as challenges takes considerable work.

In this case study, it is analyzed how to replace existing IAM tools with a cloud-based platform. Placing the entire IAM development, deployment, and maintenance processes to the cloud is an easy sell to organizations. Challenges appear during the replacement so instead of directly replacing the tools, only IAM use cases are straightforward to move into the cloud. Existing processes rely heavily on the existing on-prem IAM tools, so even if a use case was migrated to the cloud, a way for IAM to implement cloud services in a way that existing processes can continue without hindrance is necessary.

When the cloud IAM platform was implemented, the fundamental design and functionality of the tools govern the way IAM worked. Switching to a new IAM tool would require a considerable amount of change. The implementation should be modular and focus on implementing in a way that new tools can further be developed. Governance can use manual processes to develop usability and functions but the aim is to have processes as fast, self-service and automated as possible. Existing integrations with a consulting company slowed down agility, so accelerators should be built to remove the need for consulting for future processes. To achieve this, an IAM DevOps team, which is a team dedicated to IAM governance and platform development, was recruited.

IAM DevOps teams are formed by bringing people from the development, testing, and operations together to continuously deliver a product with built-in quality. During the recruitment process, emphasis was put on team members having experience from outside of IAM for new ways of working and understanding about cloud capabilities. The IAM specialists often know the product functionalities but lack experience of high-quality development and testing practices. Some of the recruited had prior development experience but limited knowledge with IAM. This was found more efficient than recruiting only IAM specialists who lacked knowledge on other development aspects.

6.2. Integration with Existing Systems

Implementing a scalable IAM solution that integrates successfully with existing systems is a complicated task. However, as is typical in the insurance industry, applying IAM to core systems is usually not feasible, therefore some degree of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

compromise is needed. Close cooperation with providers and custom development is essential to build a system that matches product scenarios. Systems based on standards like OAuth 2.0 or OpenID Connect boost interoperability and make it easier in the long term to replace parts of the product. Essential IAM functionalities should be implemented in-house whenever possible, as they constitute core parts of a system. When building IT infrastructure for digital insurance, no existing stack of modules fully matched the insurance business model. As well, little funding was available to build everything up from scratch providing only an end-to-end MVP for an insurance case.

To comply with modern requirements of IAM, core functions such as account creation, sign-in and linking existing identities were implemented within the insurance platform. There exist vendor products covering some IAM functions but were feasible alternatives. Built from scratch or enhanced with off-the-shelf products, the optimal candidate was a combination of existing vendor products. An insurance company, of size currently below 400,000 policies, acquired additional containers for troubleshooting purposes. Prospective containers were considered in case the whole system would fail and demand rise rapidly. Expanding these would require up to 5 individuals continuously, as current management of 5 could run several projects in parallel, not the product itself. Given support be no more than 4 questions, little education is needed on the default product. All available languages spanned both UI and API. Objects and attributes were easily extendable with no apparent limit.

To overcome these interoperability challenges and make the Insurance Platform more attractive since gains see development timelines until large changes can be implemented. Ultimately enabling cooperation with smaller players by offering a (partially) White-label Insurance Platform on a SaaS basis is the goal. However, this model requires a standard IAM & API as presently only conceivable by throwing functions A, B, C or others overboard. Replacing the front end, moving to a different stack, replacing education and documentation offers zero benefit aside from one central product. Currently no SCM-based hop is able to load data implementing their IAM concept on a reasonable timescale, although parts of IAM services exist with either one or the other party.

VII. SECURITY CONSIDERATIONS

As more organizations are developing digital insurance services, there are multiple aspects of building such platforms in a secure and trusted way. This paper focuses on implementing scalable identity and access management (IAM) frameworks that can provide enhanced levels of security and flexibility in terms of managing access to corporate resources based on the dynamic context of the access. IAM plays a crucial role in information security management and is often the most attacked part of organizations. Therefore, as part of a trustworthy digital insurance platform, IAM requires a strong foundation in security. The achieved results include a comprehensive IAM framework that prioritizes secure and trustworthy identification, authentication, and authorization methods with evaluations of their potential security risks. Besides, the developed IAM framework is offered as a service with easy integration points to facilitate onboarding new partners, potential business expansions, and easy use. Furthermore, as digitization creates new opportunities for growth, insurers are seeking a suite of integrated, customer-centric platforms to succeed in this rapidly changing environment. One of the key elements in enabling new technologies and business models is the ability to collect customer data and analyze it in order to offer a better customer experience. Data brought into these platforms is often exposed to data leakage and misuse, which can create harm to the customers. However, the insurance industry has essential experience handling sensitive data based on regulatory requirements protecting personal data, which can be leveraged to build secure platforms.

This paper presents the design and implementation of a trustable and secure IAM framework that can meet the regulatory requirements on handling sensitive data in the insurance domain. Furthermore, it provides principles, processes, mechanisms, and storage solutions for IAM in both cloud and distributed environments on new platforms that have been designed with privacy-by-design principles and secured risk management in mind. A key consideration in implementing IAM on new platforms is adaptiveness to diverse customers, products, and regulatory requirements. Such a need is different from most existing IAM solutions targeted toward less dynamic environments. Privacy and regulation compliance are essential yet challenging to meet requirements for IAM implementation in an insurance environment embedded in new platforms. Therefore, the IAM design addresses how to implement a scalable framework that can address various privacy requirements from customers, products, and regulations for diverse and changing environments. However, controlling access to information using IAM is often a major security management challenge in digital insurance platforms. IAM is often the most attacked part of a corporate infrastructure and requires special consideration and defense mechanisms to protect against a variety of attack vectors. Hence, considering the possible attacks on IAM in traditional, cloud, and blockchain environments, the IAM implementation leverages mechanisms to minimize defense exposure and meet regulations.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

7.1. Data Protection and Privacy

This chapter presents recommendations for implementing scalable identity and access management frameworks in digital insurance platforms. Since each insurance organization is unique in its operational processes, regulations, cultural features, and legacy environments, a one-size-fits-all solution may not work. Therefore, a modular framework is proposed that allows each organization to select components on-demand. The vendor-neutral framework enables insurance organizations to combine commercial software, open-source components, and home-grown solutions, ultimately building an IAM solution that is right-sized to meet their needs.

The framework is scoped to meet the needs of elementary IAM functions used throughout the insurance value chain. Each chosen IAM function is broken into a number of self-contained modules that provide a wire-to-wire solution. Each module contains a number of configurable components while adhering to commonly accepted industry standards and leading vendor software. Smooth integrations allow sharing of functional data between modules, building an enterprise-wide environment.

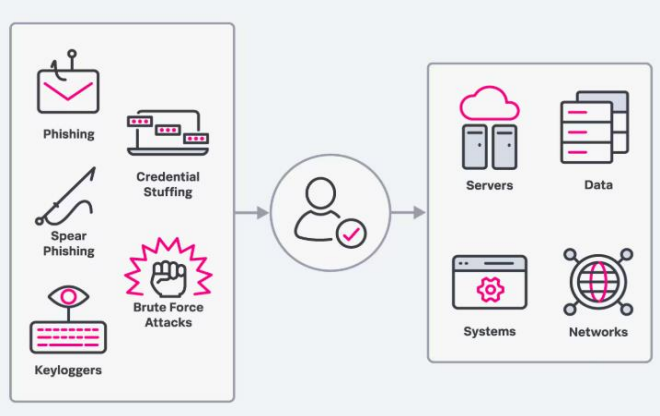

Fig 4: Data Protection and Privacy in IAM.

Recommendations for IAM strategy implementation are presented, detailing a high-level blueprint, which should eventually result in a right-sized IAM solution that evolves with the organization. The blueprint should guide insurance organizations in selecting different modules and components on-demand, ensuring coverage of immediate requirements before progressing on to more complex scenarios. A 3 to 5-year implementation plan for producing an initial IAM deployment is outlined, followed by options for expanding this deployment to cover additional IAM capabilities and modules at a larger scale. The chapter concludes with advice on successfully managing the IAM strategy implementation while maximizing the chances of success and minimizing risks.

7.2. Compliance with Regulations

Compliance with regulations and laws is a complex and ongoing challenge for organizations. Many organizations have taken concrete actions to comply with various regulations, yet gaps still remain, and compliance will never be "complete." As regulations change, new legislations come into force, and organizations grow and change, the regulatory requirements landscape becomes more complex.

External regulatory requirements typically start with a single piece of legislation: a law or regulation. A high-level description of how a company meets this requirement is. This description will contain similar items for all pieces of law and regulation. In many, if not all organizations a part of the governance charter is the Code of Conduct. This document describes the values and standards of expected behavior of an organization's employees. Separate documents can be Executive Orders, Data Protection Impact Assessments, "FATCA Due Diligence Procedures," "Know Your Customer" descriptions or Anti Money Laundering Policies. These descriptions will contain controls for various items, including the design and operation of the organization's legal compliance.

Laws and regulations almost never contain a declaration of completeness. Instead, they will contain requirement items such as "appropriate" or "adequate." This gives much freedom (and, sometimes, room for interpretation), but it also creates a challenge for organizations: "How do we know we are compliant?" Compliance with laws and regulations is like driving a car. One must start somewhere, and there is a specified destination, but roads may be missing, and road signs can be ambiguous. In many cases, legislation is created too quickly or is too vague for one or more of the actors in

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

the legal community to understand what is "okay," "not okay," or "okay with a fine." Over the years, courts create case law and fine-tune the interpretations of laws and regulations, often very much after the inconvenience has taken its toll. There are at least two important areas in which these challenges manifest themselves: (1) Developing a view on regulatory requirements and controls, and documenting and maintaining this view, and (2) Creating insight into compliance where, currently, almost all organizations run out of Excel spreadsheets and PowerPoint presentations.

VIII. USER EXPERIENCE AND ACCESS MANAGEMENT

User Experience and Access Management in Digital Insurance Platforms.In the digital age, users wish to have an intuitive but diverse experience when accessing services. In harmony with this expectation, the future identity and access management framework should provide intuitive access methods (with a focus on user experience), while also simplifying the on-demand identity and access management capabilities (with a focus on implementation ease). This section will introduce two important innovations in the future identity and access management framework, which are expected to improve the user experience in accessing & utilizing digital services in insurance platforms and ease the implementation of the frameworks without too much knowledge for overly complicated and service diverse equipment. Modern access management frameworks promise easy and convenient user access to digital services in insurance platforms. However, implementation difficulties arise when the complexity of the on-demand experience is raised, thus diminishing the user experience. In order to improve users' experience while having the freedom of intentions, an improved user access method is presented to balance users' diverse needs and platform implementers' limitations. The proposed access method introduces time and mode properties into the conventional workflow-based access method while allowing users to experience it with a hybrid approach.

In traditional access methods, access policies are designed to be use-case siting in static structures or dominant workflows considering the use of techniques. However, this could sacrifice the user experience and become an implementation burden when users' diverse needs and access requests appear, especially in an ever-changing information environment. To improve the user experience while making the introduction of the on-demand access method easier for the on-premises platform, the proposed improved user access method works with two properties including newly supported time and mode properties. Access requests over services can be recorded or tentatively inserted with timing triggers, which can also work in combination with existing user activity recording for use-case intelligent management consideration.

In order to deal with the evolving user intentions that accompany the digital business transformations for insurance platforms, an access management architecture is elaborated with the focus of proposing a hybrid access approach in which on-demand access control could be embedded into a conventional workflow-based access management framework when needed. In the content-centric application, users enjoy subscription-based digital service access which could be reverted as immediate usages of hard assets, and they would like to experience straightforward access methods. The access management framework is proposed to bear the idea of data origin-centricity and is enhanced with a workflow-based routine access method.

8.1. User-Centric Design Principles

Insurers frequently redirect their automation plans to new and updated technology. Digital service platforms characterize current insurance markets, allowing consumers to select strategies, premiums, and wagers based on comparison shopping. Digital channels also offer new data sources for risk assessments that make coverage options available for devices and property. Implementation is not as easy as it seems, as it requires swift transformation and adjustment of products, processes, business models, structures, and technology.

An organization has weaknesses when on the verge of significant change. Prevention costs tally seven missteps in this risky transformation along with remedial advice, highlighting damage control in case of belligerent forces and the importance of technology partners. Finally, agility is called for as principles regarding user-centricity, necessity, and regularization.The requirements outlined in the previous section are high-level principles based on scholarly investigations regarding the future of identity and access management on the internet without technical implementations. It is intended that in the future there will be decentralized systems that enforce and uphold these principles for identity management and access control throughout the internet.

The present section is concerned with the design implications based on exemplary implementations of some of the principles, approaches, and novel building blocks from recent research activities. Building blocks depend on browser stack code and so-called "decentralized identities" culminate in identities that enable users to prove the possession of attributes from different credentials, with anonymous credentials where no information is shared unless desired. Such objects provide global identifiers bound to real-world personal data that hold best of both worlds, operability, and agency.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

These objects can be provisioned through links to decentralized trust hubs that hold code stores. Identity and other metadata to include claims are certified using decentralized identifiers (to be stored in a distributed hash table). This information suffices to carry out access control. Security primitives for the computational core of the stack enable lightweight proofs that prove possession of credentials without revealing them, operate verifiably with intellectual property of the owner, and invoke cryptographic tokens to prove capability according to specific attributes.

Equ 3: Access Latency Reduction Rate (ALRR).

$$\text{ALRR} = \frac{L_{\text{baseline}} - L_{\text{IAM}}}{L_{\text{baseline}}} \times 100$$

- L_{baseline}: Average access latency before IAM implementation
- L_{IAM}: Average access latency after IAM implementation
- Quantifies performance improvements due to optimized identity workflows or federated access.

8.2. Balancing Security and Usability

The demographics of modern society push us toward an online existence. Modern society is racialized according to the Structuralist notions of socio-economics, ethnicities, and so on. Personal data are extracted based on these characteristics, and companies and countries capitalize on these data extracts. Individual-data rivalry is assumed by many researchers. However, this rivalry on an abstract level can be easily broken by the very algorithmic process that powers the automatization and efficaciousness of online systems, as an essential basis for this competition is an assumption, i.e., a Guassian noise around some average category is produced by some self-fulfilling mantra categories such as “one-size-fits-all,” “more is better,” and “demogados.” Corporates become (quasi-)creditors of individual data and laser individualized enslavement contracts are executed between data and a third party (the insurance company). In the age of digitalization, actors traditionally seen as adversaries, such as data/insurance-write and -receivers, merge into monolithically dynamic, agent-based ecosystems.

The exact form of the consent is now up to the automatic contract drafting and passing services. Non-linearities and the ability to process intractable complexity render individuals unelected in insurance markets. It is being implemented by off-line economic based actors such as human resources, commercial agencies, and diary-based services under a rubrique. The architecture enabling all these metamorphoses on modelling powers is quasi-open source. This allows the community to converge to an optimal race to the bottom profile encoding. This writer’s non-discriminate thought limits its empathy for nondiscrimination. The horrid and weightless racial-faked effects lead to an outrageously depressed community-effort to this tune. Solutions derive from recency modelling branches of the community, but context and latencies offer unintegrated additions from the dungeons.

Credential Stuffing Attack. Data breaches expose user’s credentials like usernames or email accounts and the associated password hashes with a narrowed cryptographic hash algorithm. If the password hashes remain unsalted, the abducted credentials become a devastating threat because many people reuse their username password pairs across services. Attackers apply credential stuffing attacks with existing stolen credentials to readily hack into the targeted services. Credential stuffing concerns the reuse of legitimate user credentials while brute-force attacks concern the use of valid but randomized username password pairs.

IX. CASE STUDIES

Digital insurance service is made possible with more ecosystems of third parties, which causes demands to share digital identities and authorizations. Stateless Simple Web Service Protocol based on a unique UUID and endpoint URL is proposed to improve on OpenID Connect. A scalable identity and access management (IAM) framework is implemented to support both the centralized approach with the OAuth 2.0 and OpenID Connect based third-party IAM server and the proposed distributed approach of sharing digital identities and authorizations with partner parties. Gateways of access management are used to process IAM calls between partner parties and their third-party IAM servers. Digital identities and corporate authorizations are shared with partner parties and include authorizations to grant further access to partner parties. This IAM framework is applied to the representative Sumi-i insurance platform.

Currently, IAM servers are centralized within each organization. Digital identities and authorizations are not shared with other organizations to protect privacy and for security concerns. Each user here must create a new account to a service provided by another organization. Newly created accounts only include basic information such as name, organization and role. Access to resources is granted generically by allowing to know the type of resources without knowing it originally. Access to resources of other organizations is a security concern. Every login attempt to access resources are verified mainly based on whether it had been previously granted. Thus processing of user requests takes much time. Organizations cannot take advantage of open ecosystem of service providers.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

To share global or federated digital identities and authorizations among parties for cross-party insurance services, the stateless simple web service protocol is proposed, which improves on OpenID Connect by using UUID as a unique content identifier and universal endpoint URL. Security of the web service calls is ensured mainly with HTTP header metadata. Digital identities and corporate authorizations are protocols for sharing personal information of the digital identity called `Account' (A) and the access management frame called `Smera Insurance Manager' (SInsM) that also includes access decisions for a company or organization. To implement the IAM protocols as an IAM framework, a stateless design pattern using SQLAlchemy is first applied as every protocol calls either 1 or 0 methods for scalable processing of requests.

9.1. Successful IAM Implementations in Insurance

The participants comprising insurance companies, banks, social media companies, and telecom operators must justify their clients' identities promptly and with fair effort, thus thriving based on the client knowledge safety pillar in this approach. Ad-hoc groups are formed in a transparent manner, allowing pseudo-anonymous transactions where constructed reputations share risk assessments against fraud. Social activities and certifications originate in alternative legitimacy paths, thereby establishing relations to the relevance of an identity, all without the need of a trusted party. In consortium insurance models, consumer and industry representatives devise the trusted regulator, its rules and conditions for evidence, along with the compliance of client inquiry requests and fraud investigations.

User identities generated in social media companies and recurring telecom floor accounts contain ample knowledge of settled consumer identities but have to be cross-referenced among datasets before revealing sensitive knowledge. By open Consent Managed identities (CMIs) generated, among others, by such pooled assurance mechanisms, this recommendation can be fulfilled. As an Identity Trust Trust, the protocol infrastructure managing the gathered identities mitigates fraud and entitles transactions having a legitimate social and economic basis with incentives. It also handles regulatory jurisdiction in an acknowledged manner. In this open and transferable identity model, citizens retain control of their data and can alter it in hand-held personal information vaults while gaining full knowledge.

9.2. Lessons Learned from Failures

The subsection addresses challenges and failures in implementing identity management frameworks in digital insurance platforms. These experiences offer valuable lessons for future endeavors. Instead of focusing on ideal conditions or theoretical scenarios, these lessons are derived from failed attempts that adequately match the framework's specifications, technology approaches, and architecture principles. By challenging norms and revealing potential dilemmas, these lessons can enhance discussions on launching similar projects. It is essential to adapt and prepare solutions upfront to increase the chances of success in comparable settings.

Using the Identity Management Solution Architecture (IMSAs) framework and design notation as a discussion and design modeling tool for an IAM system, industry experts were engaged to create an IAM architecture for the Health department of the government of Canada. Initially, several concepts in the domain of IAM architecture were successfully redefined. However, despite the workshop's organization, discussion, and feedback meetings with interested parties, the initial enthusiasm and interest faded, and no further feedback or involvement occurred.

The initial ownership and interest from some stakeholders evaporated in an unstructured manner, leading to numerous implicit assumptions in the architectural development. Despite efforts to include technical documentation and design validity regarding current and future second-generation IAM systems, the comments and feedback were not what was expected. After 6 months, little progress was made, suggesting the need for a more structured approach and more check and balance moments in the project. Regular updates and insights on the current state of the evolving IAM architecture should have been maintained to increase ownership and interest among other stakeholders. Academia's role in projects should not solely be to deliver output, but to actively seek involvement, keep everyone accountable, and involve less motivated stakeholders in discussions.

X. FUTURE TRENDS IN IAM FOR DIGITAL INSURANCE

The inclusion of secure identity management has become a top priority for businesses looking for end-to-end security from the packet level all the way up to the application level, preferably through an integrated approach. There is a growing interest in exploring how identity management and access management strategies are used in practice by companies. Meanwhile, digital insurers want to draw on accumulated tools. They hope to utilize understanding and analytical methods to bolster identification and access processes, just as telecommunication companies have done by transferring multiple services to a single access point. This paper embarks on such an expedition. It is an invitation to probe how telecommunication and email services have handled the transition; to comprehend motivations, choices, selections, obstacles, and pushing forces; and to formulate a list of questions for digital insurers to ponder.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

Today, users have many different accounts, which often require different credentials. Risks of forgetting passwords, losing devices, or unauthorized access are common. Though these assumptions normally are acknowledged, a clear definition of the problem is not easy. Today there is no identity management provider or tool in which the user could administer all accounts. Attempts to build such a service have either custody issues or content dependencies.

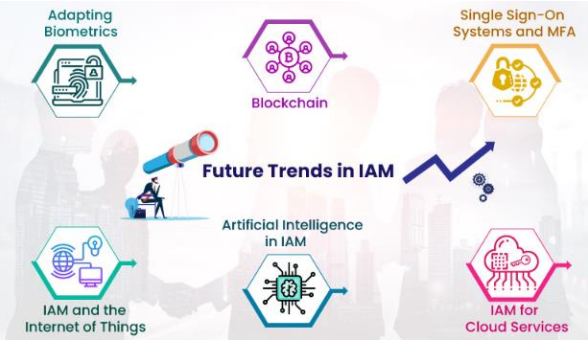

Fig 5: Future Trends in Identity and Access Management.

Smartphone users may operate with one or two biometrical key movements, which subsequently generate user identification and password retrieval. Hardware manufacturers contend this is not done with user input; a big user acceptance model and marketing efforts will likely follow. The problem definition resembles a design endeavor. In practical terms, it is a matter of defining a system that obfuscates account storage without putting total custody on an external agent, and that defines a method for tracking credentials in multiple stores with respect to security and privacy.

10.1. Emerging Technologies and Innovations

Additionally, in the case of re-insurers, conventional insurance has undergone an evolution and has begun to gain new forms. With the rise of cryptocurrencies and blockchain technology, the emergence of financial products and services based on crypto assets and blockchain disinclined investments has resulted in new market demands, one of which is the need for protection against risks such as loss of private keys, misplaced funds sent to an incorrect wallet, and hacks or exploits of smart contracts. With this demand arise new risks and challenges stemming from the infancy of blockchain technology and crypto assets. The introduction of novel insurance services and products such as a decentralized way to insure against hacks or losses of digital assets has begun to emerge. In addition, centralized insurance service providers are also trying their best to extend protection to this new realm. Current insurance services based on legacy technology are facing challenges due to the unique nature of its underlying technology which requires the adaptation of existing insurance architecture or even the ground up construction of a new automated and streamlined paradigm.

Token-based insurance solutions on blockchain allow the encoding of measurable and tradeable insurance coverage in the form of tokens and offer insurance services that transform the existing insurance industry in many aspects, including product coverage that caters for new risks, underling process to accept underwriting requests, assess claims, and dispute resolution that have become more automated and seamless, on-chain workflow to track the whole insuring or claims processing, etc. Existing work describes several implementations of token-based insurance solutions and comparable characteristics, such as core process, product coverage, token classes and token functionality. But the underlying blockchain technology and the difference in design ideals are not discussed, which is of particular importance because it illustrates the way in which such insurance solutions could evolve in the future. Token-based insurance solutions on blockchain garner attention from both academia and industry, with several existing insurance services based on blockchain technology. The unique nature of blockchain technology and crypto assets renders this emerging industry different from conventional ones. On one hand, innovative insurance solutions utilizing features of blockchain such as automatic and trustless insurance products are proposed. On the other hand, a risk-centric approach to protect new risks arising from the infancy of blockchain technology and crypto assets has emerged recently in different approaches.

10.2. Predictions for the Next Decade

Ten years from now, the identity and access management (IAM) frameworks implemented in large-scale digital insurance platforms will undergo transformation and refinement processes. As insurance companies—and fin-tech companies in general—adapt to new regulatory frameworks, the proposed and implemented IAM frameworks will also evolve. Only those companies capable of quickly and efficiently adapting IAM frameworks and regulations will survive competition. This is especially true in digital businesses. Six prediction points regarding the evolution of IAM frameworks are made.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

In the 2030s, the phrases “privacy by design” and “identity by design” will be used regularly. Current IAM frameworks tend to build de facto monopolies on users’ identifiability. Insurers or companies need to gather the data they need once during the onboarding process. However, they will not become unidentifiable. Instead, strict regulations for “minimal collectability” will be passed worldwide. Video bank account onboarding will make users’ identifiability indisputable. As machine learning (ML) technologies advance, identifying users will become easier without traditional documents, using only soft biometrics like video streaming or voice. Insurance companies should act preemptively. Under users’ control, insurance-type trust networks will start to emerge, allowing users to organically reconfigure privacy-centric use cases. Fin-tech companies must passionately educate users regarding their rare privacy and reconfigurability rights.

More intelligent and fine-grained IAM systems will arise. Currently, IAM approaches are coarse-grained, meaning the systems cannot govern the whole deed of users in multidimensional ways. The emergence of a “supervisory identity layer” that governs events that occur in other services and IAM systems is anticipated. Insurers should consider using identity-driven design rather than activity-driven design. The latter focuses on affordances to identify user interactions instead of desirable identities users want to adopt. While activity-driven design can cause misunderstandings, identity-driven design better portrays desirable interactions based on user needs. Unfortunately, it is not easy for any company to be capable of supervising any activity of users. In the 2030s, there will be either companies with such power or widespread public distrust and anger towards either those companies or ungovernable societies. Identity agencies focusing on pseudonym audibility and linking will be widely introduced. Users will utilize them to build complex multilayer identities under data custody. As far as the roles are “technical” types, such protection will be technologically guaranteed. Although dubious claims may be made, tokens can be fed to these super IAM systems for obscured, reconfigurable, digital identities. If it suddenly becomes a cabal controlling the industries, new generations of IAM approaches will succeed in identifying companies in 40 years.

Fig 6: Identity and Access Management Frameworks in Digital Insurance.

XI. CONCLUSION

This research paper studies the existing architecture of an insurance application to identify its advantages and disadvantages in order to design a new scalable security architecture. The new architecture is based on Identity Access Management, Access Control List and Role-Based Access Control. The use of IAM frameworks promotes scalable security architecture to become the standard in enterprise-scale solutions. As the digital channels for viewing insurance solutions grow increasingly provide a variety of services and platforms, the choice of digital solution turns critical to the successful implementations of digital Insurance solutions.

The new architecture was implemented on microservices, message driven architecture, and cloud easily able to develop and deploy the solution on hybrid cloud providing the flexibility to scale its infrastructure. This paper describes research that implements a scalable security architecture for microservices. Its focus is on providing Enterprise Scale Security for a digital insurance application leveraging IAM Frameworks, ACL, and RBAC Policies. Solutions using IAM Frameworks, ACL, and RBAC refer to standard Security First solutions in securing any applications. Applications with such a security model have been adapted into the standard security solution in the insurance application space. This paper also addresses how this architecture can be built on various advanced developing technologies such as serverless microservices, Event Driven Architecture, Reactive application models, and cloud platforms. This scalable architecture has the potential to help large digital insurance implementations benefit customers.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 12, December 2020

DOI 10.17148/IJARCCE.2020.91224

REFERENCES

[1] Karthik Chava, "Machine Learning in Modern Healthcare: Leveraging Big Data for Early Disease Detection and Patient Monitoring", International Journal of Science and Research (IJSR), Volume 9 Issue 12, December 2020, pp. 1899-1910, https://www.ijsr.net/getabstract.php?paperid=SR201212164722, DOI: https://www.doi.org/10.21275/SR201212164722

[2] Data Engineering Architectures for Real-Time Quality Monitoring in Paint Production Lines. (2020). International Journal of Engineering and Computer Science, 9(12), 25289-25303. https://doi.org/10.18535/ijecs.v9i12.4587

[3] Vamsee Pamisetty. (2020). Optimizing Tax Compliance and Fraud Prevention through Intelligent Systems: The Role of Technology in Public Finance Innovation. International Journal on Recent and Innovation Trends in Computing and Communication, 8(12), 111–127. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11582

[4] Mandala, V. (2018). From Reactive to Proactive: Employing AI and ML in Automotive Brakes and Parking Systems to Enhance Road Safety. International Journal of Science and Research (IJSR), 7(11), 1992-1996.

[5] Ghahramani, M., Qiao, Y., Zhou, M., O'Hagan, A., & Sweeney, J. (2020). AI-based modeling and data-driven evaluation for smart manufacturing processes. IEEE/CAA Journal of Automatica Sinica, 7(4), 1026–1037. https://doi.org/10.1109/JAS.2020.1003114