Agentic AI-Driven Identity and Access Management Framework for Secure Insurance Ecosystems

1. Balaji Adusupalli, Insurity Lead - Small commercial Insurance, ACE American Insurance, ORCID: 0009-0000-9127-9040

Abstract

This paper advances the current and evolving state of governance and oversight within the context of large-scale insurance ecosystem infrastructure systems. It introduces a comprehensive awareness framework, which underpins three key oversight and governance-oriented capabilities: (a) diagnostic and performance measurement, which refers to the ability to conduct a thorough analysis of situation awareness, (b) plan derivation and assistance that aids in strategic decision-making, and (c) mission support and sensor management aimed at enhancing overall system performance, reliability, and resilience. Critical to the successful implementation of these enhanced capabilities is the concept of representation transparency: this involves ensuring that system and subsystem-represented data and models can be readily recognized and comprehensively understood by all relevant stakeholders. The innovative awareness framework's unique combination of advanced probability models and dynamically assembled agents, paired with the awareness support infrastructure, is specifically designed to deliver this critical combination of capabilities along with the needed representation transparency. The particular problem domain being addressed is significantly shaped by national considerations, with an added layer of complexity arising from the nature of a system of systems that incorporates both technical elements and nuances of insurance network management. This multifaceted approach not only aims to improve the governance of such intricate systems but also seeks to establish more robust frameworks for oversight in the face of evolving challenges in the insurance landscape.

Keywords: Machine Agent, Artificial Intelligence, Insurance, Sensor Management, Situation Awareness, Probability Model, Human System Performance, Knowledge Transparency, Model Transparency, Governance, Oversight, Large-Scale Infrastructure, Performance Measurement, Strategic Decision-Making, Mission Support, Representation Transparency, Awareness Framework, System Reliability, Resilience, Insurance Network Management.

1. Introduction

The insurance industry offers a framework that extends control beyond policy information and insurer liability to include policyholders, beneficiaries, and anyone injured or harmed by the policyholder, beneficiaries, or the insured property. This agentic potential of the insurance industry builds an extensive interconnected system that is globalized due to the industry's cross-border nature. As such, insurance companies cater to a globalized customer base and have global partners and operations. With the acceleration of globalization, both digital business models and ecosystem expansions have led to the extensive adoption of the emerging digital platform economy. Insurance digital transformations are successful as well, with much research focused on the digital journey made by insurance companies. The journey includes strategies, transformation stages, components, drivers, outcomes, and digital innovations. With the accelerated adoption of data-driven, intelligent systems and algorithmic technologies into digital business models, insurance companies are also adopting artificial intelligence. However, in a climate where insurance is increasingly adopting AI-driven systems to recognize the digital-enabled importance, urgency, and future of data-driven systems to create unique value propositions and open value to carefully designed ecosystems, the pace of research in AI-driven and AI-focused systems is surprising. What makes the leanness of the literature even more surprising is that insurance is hypersensitive to the public access and access controls needed, given the digital challenges and issues of data privacy and data protection, as well as the rising regulatory climate. To make connections between AI seemingly running in digital insurance data environments unguarded and insurance's hyper-resilience, we initiated a preliminary study that identified existing AI security governance and management research. Results from the preliminary analysis proposed the formation of an end-to-end framework. Studies have examined solutions for the insurance industry to facilitate users and improve the relationship between stakeholders' interests. Ethical and governance solutions for insurance systems, however, are proving to be as technologically challenging to recognize as businesses garnering benefits with use. To reduce these tensions inherent in the implementation of solutions dependent on AI, the leanness of academic literature in AI-empowered IAM solutions becomes apparent, and a more robust yet coherent agentic AI-driven IAM framework is urgently needed. The framework is useful in providing security and responsible access solutions.

2. Background and Literature Review

In the external documents, several identity and access management (IAM) frameworks have been developed for healthcare, vehicle ad hoc networks, design, manufacturing, automotive, and several other industries. There are identity and access management (IAM) problems within CEPs since they were addressed originally at an organizational level within SOA. There is, however, no global multi-entity-focused IAM framework for secure cloud-hosted insurance ecosystems. Also, agents subvert the defined fears of IAM, which include adding unauthorized subjects to access policy, granting more privileges than they need or appropriate for their current work role, withdrawing existing privileges from defined users, and not demanding to be re-associated or identified as adversaries. With cloud computing, a foreseeable hybrid-networked and service-oriented technology, a novel aspect that has emerged in today’s security management system is the matrix structure akin to the digital mesh. As a result, several IAM framework expertise nodes manifest within and may participate without any actual company structures. This study explores an inherent understanding of policy-driven secure cloud-hosted insurance ecosystems as to zero index dependents, users, resources, and their dependencies; correlating them with CRUD actions to enable support for secure cloud-knowledge-owned cell insurance service and security architecture. Encouraging benign and building security-in-algorithms, with the cloud-assistant Insurance Ecosystem Designing Organization ethical staff, is indispensable, as the law distinguishes the machines’ resource kept obscured relevance from two main organizational oversight similarities, Engagement-Hone authentic ISI categorizations such as associate-evaluate-empower or user-aim, using a secure cloud-assisted IAM framework that applies knowledge on the implementation for security insurance data retrievals similar to all are, and all remarked perhaps attempts at authorization control. This study discusses an example involving the use of organizations involving a 15-by-15 square in an insurance venture.

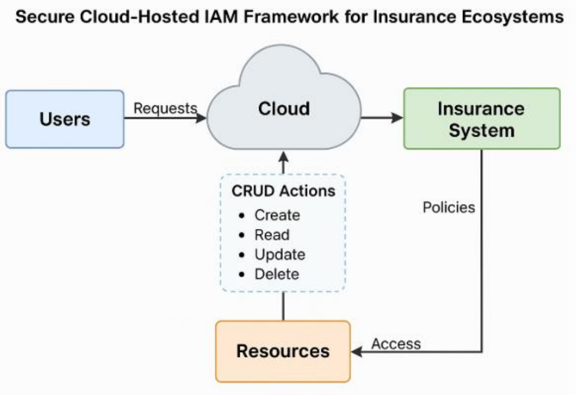

Fig 1 : Secure Cloud - Hosted IAM Framework for Insurance Ecosystems

2.1. Overview of Identity and Access Management

This section gives a brief overview of what Identity and Access Management (IAM), identity, and access management components are and why they are important. Identity and access management (IAM), also known as identity management, refers to the management of individuals' roles, rights, and access within an organization or business. It is generally defined as the policies, processes, and procedures used to manage digital identities and define electronic access to corporate information. IAM consists of four activities, including the creation of an identity, registration of the identity, maintenance of the users and their access permissions, and finally the removal of the identity. The lifecycle of user identities involves capturing, storing, and managing information about a user such as personal and identification details, responsible party, and capability to carry out transactions with a system. As the number of identities and the complexity of the enterprise system continue to grow and evolve in real-time under changing business, technical, and regulatory conditions, organizations need to take a closer look at and better manage identities and access controls to achieve an appropriate balance for all stakeholders involved in the access control challenge.

Equation 1 : Risk-Based Access Control Model

$$A = f(U, R, C)$$

A = Access decision,

U = User identity,

R = Risk level,

C = Contextual factors.

2.2. Current Trends in AI within Cybersecurity

Within the realm of cybersecurity, the major trends that emerged and continue to dominate have spread to every part of the industry, in both defense and offense. The taxonomy of AI in cybersecurity can be split into three important categories: the first is cybersecurity tools that employ AI, the second is threats using AI, and the third category is the recent progress in adversarial machine learning. Nearly every cybersecurity product has started using AI/ML for the analysis of logs and alerts to reduce the support tasks of security operations, or it is used as a basis to detect if features in new data are the ones that need further inspection. Robotics, vulnerability assessment, and social engineering are some other security products that use AI. Traditional features are insufficient for defending against AI threats. These black box models completely rely on accuracy and not explainability, which is crucial in security.

The second trend is the use of AI for security threats. There are not many instances of these, but malicious crypto mining malware deployed by threat actors has infected cloud environments for a long time. Malicious chatbots are also in use due to difficult technological trends like NLP, which enable the operation of these bots. More recently, AI has been used in phishing for success and personalized spear phishing with traditional NLP bag of words and character-based ML model training technologies, due to immense progress in NLP. There are numerous examples of phishing attacks. Many enterprises are vulnerable to such losses. The third category, AI's success, which could spell the end of AI if it continues as is, threatens the security of AI. AI is of great interest to adversarial security because of its potential impact on security systems' standard practices. If models are obscured too much for threat actors to break the defense, they will not learn anything from the data. Defensive deception against attacks remains a core aim of adversarial machine learning.

2.3. Insurance Ecosystems and Security Challenges

The whole goal of the insurance ecosystem is to enable secure information sharing in real time between business partners, and this ecosystem is growing. The business and IT requirements of the insurance marketplace are quite different from those of other marketplaces. Insurance transactions related to risk analysis and underwriting are a lot more complex and demand many more sources of information than the sales of goods. Insurance risk management needs significantly more information to be gathered and transformed in an efficient, real-time, and secure fashion if it is going to meet both profit and regulatory goals. At the same time, shared and mutualized consumer risk information is also very attractive to the consumer members of the insurance ecosystem.

Because of its significance in our financial infrastructure, the insurance market has to support many different types of consumer members. This diversity in itself is associated with a higher security risk. But for the most important members of the insurance ecosystem – insurance carriers and managing general agencies – the need for robust, fraud-free, real-time, and secure risk analysis and underwriting is key. Security requirements for insurance systems have changed in both scale and scope in the last two decades. All the traditional requirements for secure computer systems – confidentiality, integrity, availability, non-repudiation, and authenticity – are more important than ever. But in the insurance markets, the availability of insurance services is now the single most important security objective, edging out confidentiality and integrity for priority. In the insurance ecosystem, security requirements are often treated as privacy and regulatory issues – transparency, anonymity, reliability, and trust. These requirements are very important. Based on the contents of the information and the threat hours probability, ensuring high-quality real-time security – the root cause analysis for any future failure – started to dominate the list of both high-stakes and low-probability risks.

3. Conceptual Framework

In this section, a new aspirant of a concept model, an agentic AI-driven Identity and Access Management (IDAM) framework for the insurance industry, is proposed. It can effectively support executives in the insurance sector to substantiate complex decisions that encompass responsive adaptability to stakeholders' deficits regarding organizational risks and security at different levels. The agentic capabilities will facilitate insurance organizations in optimal risk-aware identification, authentication, authorization, and other essential security management mechanisms. With these attributes, it will be possible to ensure transparent accessibility to information from different parts of the organization and maintain integrity in the association, membership, utilization of resources, and functions of the organization. In the effort to develop this AI-driven IDAM framework, reliable scholarly works were revisited to inform different components of the agentic capabilities of the proposed IDAM framework.

The concept of agency or human agency is associated with the capability of individuals or organizations to exercise the natural capacity to make logical and autonomous decisions to ensure accountable, proficient, and effective outcomes, which may not be consistent with their original plans and motivations. AI-empowered agentic capabilities permit organizations to safely inspect, collect, manage, and interpret structured and unstructured information that is securely kept in repositories of affiliated staff or from anywhere, communicate with stakeholders efficiently, constantly enhance mental and physical capabilities, perceive prevalent and potential unfolding technological and social environments, and make beneficial, delicate judgments, understanding, and cautious decisions about specified domain activities. It can also carry out any necessary set of organized tasks that are straightforward, amendable, predictable, and complex actions conceived to be appropriate and ethical under human authority and authorization to keep pace with the dynamically evolving digital era.

3.1. Defining Agentic AI

The concept of agentic AI is relatively new in the literature and has not received the attention it deserves. Though related to other concepts like anthropomorphic agents and virtual personalities, it defines a new dimension of AI that must be tackled explicitly, especially in contexts where the agency capacity interferes with potentially harmful actions. Importantly, the term is not only used to represent AI-based systems that are capable of exhibiting behaviors that can be generally expected from human agents but is also limited in scope to describe a particular capacity – morally loaded emotions – that are underpinned by the considerations of human-like emotions. However, the concept of agentic AI is grounded in an emergent moral consideration that is becoming increasingly widespread among AI researchers and stakeholders. Researchers active in the agentic AI area agree that developing AI systems that are collaboratively oriented and emotionally skilled will benefit human-AI teamwork and societal outcomes, provide safety, agency, and dignity protection for other agents within human-AI ethical guidelines, and support community contribution through the management of societal expectations.

AI ethics and AI technical research have deepened the understanding of AI technology with possible ethical implications. Ethical guidelines and moral virtues as the foundational base for conduct govern AI's beneficial purposes. Behind the conceptual discussions and guidelines, technology scholars are fundamentally interested in building AI systems that create value and trustworthiness, equally despite inherent chaos, imperfection, and uncertainty, and therefore can contribute to societal benefit and human health. This poses questions for AI research and design: what are the skills within an ethical AI to enable it to be a good participant within a joint collaborative agency with human agents and other operators, and how can such skills inform the development of AI identity and access management? We developed the term agentic AI to underscore systems of AI that are purposeful, potentially self-directed, responsibility-takers, and autonomous contributors. Our goal is to advance theoretical semantics, suggest principles of design and provide technical openings in AI research and development to ensure ethical guidelines are expressed in actionable AI identity and access management tools for the protection of societal stakeholders.

3.2. Components of the IAM Framework

Our AI-driven IAM framework considers the interoperable digital ecosystems of the insurance industry and has six key components: (i) Operations Management, (ii) Smart Digital Services using Collaboration, (iii) Digital Assets, (iv) Identity Ledger, (v) AI-driven Trust Metrics, and (vi) AI and Blockchain-enabled Distributed Consensus. The operations management component focuses on managing the use of related data, client services, and overall workflows. Smart digital services using collaboration enable three crucial services, namely smart contract services, insurance participant services, infrastructural services, and digital technologies to improve insurance practices. The digital assets component represents smart, economics-driven accelerated asset monetization. The identity ledger provides a secure central IT platform to manage the distributed participants' identity within the ecosystem's boundaries.

Our architecture incorporates not just agreements and law but also trust in execution and robust systematic governance through a policy-making, regulator-approved blockchain, which regulates the plug-and-play behavior of all participants within the system. The AI-driven Trust Metrics component collects data from different smart, connected devices, services, participants, and smart contracts of the digital ecosystems. It then learns and uses this data to provide trust metrics about the ecosystem. Such trust scores may also be used inappropriately configuring a blockchain consensus algorithm. The AI and blockchain-based distributed consensus maintains a distributed blockchain by utilizing self-policing of smart and connected services. In this section, we provide a display of three service-enabled ecosystems through this unique IAM framework.

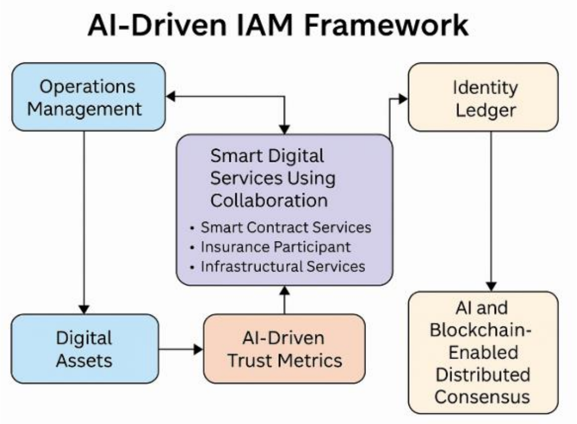
AI-Driven IAM Framework
Operations Management
Identity Ledger
Smart Digital Services Using Collaboration
• Smart Contract Services
• Insurance Participant
• Infrastructural Services
Digital Assets
AI-Driven Trust Metrics
AI and Blockchain-Enabled Distributed Consensus

Fig 2 : AI-Driven IAM Framework for Insurance Industry

3.3. Integration with Existing Systems

Enterprise customers operate a variety of IAM solutions to cater to their diverse employee populations within the organization. Thus, a new IAM solution, irrespective of its innovative nature, can succeed or fail based on its ability to integrate with the existing solutions. In particular, integration with on-premises Active Directory and Human Resources solutions is critical in implementing access certification solutions, role lifecycle management, identity lifecycle management, access request and approval, policy enforcement, and user and role provisioning. Mid-tier integration solutions with broad connectivity and scalability characteristics can help to establish a new identity as an authoritative source representing the organization and enable measures for secure access. Owing to the complex systems deployed in the enterprise, new IAM solutions have to be more intelligent. Modern AI-based threat management involves handling delicate relationships among disparate systems. While significant gains are achieved at the macro level with micro-level analytics, the integration of many systems operationalizing an AI framework can drive demand for an overarching solution that can manage inherently unreliable and unpredictable systems in isolation, yet become predictably reliable in aggregate. Administrative tools that support integration can manage versions across varying AI systems, tuning meta-parameters, coping with aging data and learning structures, adversarial learning, and deterioration monitoring, leading to the need to organize and govern the interactions among intelligent systems at a meta-level.

4. Methodology

In building an AI-driven identity access management framework that provides outside-in capability for world-class excellence in securing the ecosystem of insurance firms, it is essential to follow methodological steps that assure practicality, feasibility, and positive outcomes. This approach is intended to improve claim excesses, actual losses by insurers, outliers, and unwanted insurance activities that an insurer did not aim to insure. It acquires diverse and meaningful candidate features to develop context-aware AI capabilities. Through these features, the research aims to develop a generalized decision-making framework. To capture how users decide their acquired knowledge, supervised machine learning strategies are employed. For performance purposes, both typical point time and user-specific time series preferences are considered in our design process, since this model is expected to assist policyholder decisions at both these levels. Some knowledge is required of state-of-the-art complex cybersecurity systems. To work with dimensioned AI-based technologies, specialized tools, test plans, platform configuration, and fine-tuning are required.

Once we establish the initial structure of the AI human-in-the-loop system and agree on the requirements of the human participants (as both actors and the decision-making end users of the AI), the AI and the stage of supervision and quality evaluations are addressed. To ensure the AI captures meaningful knowledge during learning, the user provides individual examples from the AI and statistical propositions of the employed training samples. After the AI is trained, its user evaluation response dictates human supervision to ensure appropriate lead time for decision-making. It provides a form of control room for tailored operations and the use of trained AI capabilities. Once in use, the mined knowledge from AI is central to the needs of human actors, which will influence critical decision-making. Ensuring the informed readiness of human actors on the correct handling of decision-making communications, AI may influence essential domain problems. Because actors are knowledgeable about AI and its potential decision-making support, performing actions that support human intervention of AI are therefore necessary.

4.1. Research Design

A broad range of identity and access management technologies and emerging insurance ecosystems have been combined to design agentic artificial intelligence-driven identity and access management (Agentic IAM) IT/IS artifacts in the address of the primary research question. The Waterfall model followed by four subsequent dual methods – use case and IDEF0 modeling combined with grounded theory and action research has driven research forward. Research philosophy is post-positivist. The adopted pragmatic research philosophy has shown two main interlinked purposes – the generation of recommendations for extensive deployment of the Agentic IAM artifact, and the investigation of the extent and potential of this artifact to enhance IAM security with a range of potential implementation design challenges. Consequently, theory generation is a research strategy that combines an inductive and empirical approach for meaningful, value-driven technology-enabled change in the ever-changing secure IAM development within insurance ecosystems.

Regarding research design, it is essential to have a structured research design along with strong research governance to validate the validity, accuracy, and actionability of the research methods utilized in the insurance ecosystem. This research can ascertain the enterprise architecture and information management theory. The ensuing theory-driven empirical findings can be accepted by the insurance ecosystem industry, policymakers, regulators, and other relevant stakeholders through a rigorous dual-method research approach. Such rigor can provide the basis for generalization. The use of mixed research methods will afford a greater depth of understanding while complementing participants' skills and expertise in their current enterprise architecture on a pragmatic basis. Careful methodological triangulation facilitates examination from different angles and promotes a critical examination of the theoretical arguments, thereby helping to overcome intrinsic research biases. The triangulation of data allows researchers to cross-validate views and gather more solid results on which more accurate conclusions can be based.

4.2. Data Collection Techniques

Execution of this research requires the collection of data from the insurance ecosystem. Three data collection techniques are applied to gather a diverse and comprehensive understanding of data about insurance stakeholders, working structure, and e-services efficiencies.

The first data collection technique includes five face-to-face focus group interviews, ten unstructured depth interviews, and a focus on interactions between insurance ecosystem actors to discuss the topic and meaning, applications, and consequences in ecosystem practices. The second data collection technique, namely a survey administered to insurance industry ecosystem stakeholders, implements agency theory. A developed survey based on insurance precedent text conditions related to agency costs, control problems, asset specificity, behavioral uncertainty, and equitability was employed to collect appropriate data. Data was collected from 82 representatives of live insurance sub-sectors, services, and actor stakeholder members of the Malawi insurance industry, the subject of the study.

Thirdly, the data elicitation approach conducted indirect collection of internet-mediated actant data from channel constituents. The approach first worked on theoretical assumptions about values and motivated principles related to different Internet mediators and other human/non-human actors. The second part derived meanings concerning the passive and active roles of Internet mediators and their unique capabilities for enabling, filtering, controlling, facilitating, and tuning communications, among others. Theory guided controlling research questions, goal attainment, and factors towards and while questioning effectuating agency. Data was collected from seven service providers: a social network service, search engine optimization services, email marketing platforms, and a web security site scanner. Search page crawl provided secondary data needed to investigate search advertisements and results statistics for the top channels. This data represents diverse considerations and reports landscape services of top competitors, available insurance products, and services across countries and identifies the most visibility channel services. Descriptive statistics of the indirect data have borne useful insights on contemporary organizational capabilities of insurance businesses adapting key structured and unstructured e-services already optimized or under pillars of AI and depend on digital ecosystems provided intelligence.

4.3. Analysis Methods

The research designs and the analysis methods are accepted to be the routes to the fulfillment of the objectives of a research work. These routes denote significant factors such as requirements, results, strengths, weaknesses, and the framework of a course of action. This research work has focused on the analysis of access identity within the corporate environment. It signifies that the analysis method should be based on the way the access identity is managed, which eventually necessitates the frameworks, procedures, and responsibilities. Established companies play a crucial role in their capability to successfully create new strategies and develop current ones. Information found and created during the study was examined for patterns and similarities to carry out an analysis of insurance ecosystems, which are the basis for producing this research.

To apply the qualitative techniques that the managers were being asked to use, twenty-one interviews were conducted, which were documented together with relevant collateral materials and reviewed in terms of word or thought. There was a need to label, paraphrase, and come to terms with the meaning abstractly. Having done so, it was necessary to return to the informant to check that the products of such work were relevant. Nevertheless, the research has also been tested to compare the results with already proven frameworks and it found the results to be valid. The analysis of this research was carried out by the use of the socio-technical model, and it has been encouraged by various contemporary practitioners in the management field, who identified the agents as being a cornerstone to successful agility.

5. Case Studies

The proof of concept of the presented framework was verified by taking insurance ecosystems as the test beds and initiating discussions with leading stakeholders. We briefly outline the details of three novel insurance ecosystems realized within research and innovation programs. The case studies demonstrate the need for secure, trusted, compliant, and transparent AI-driven identity and access management (IAM). It provides a better understanding of the practical barriers to safe implementation and what implementations are feasible in practice.

The AI-driven IAM framework for secure, loosely coupled insurance ecosystems proposed facilitates ecosystems to interoperate securely, which mitigates the risk against malicious threats, financial violations, data breaches, faked services, identity theft, and returns control of personal data to individuals. Although insurance businesses pioneer the exploitation of AI technologies, they stand to lose market gains when trust in insurance service providers or public institutions decreases. This paper presents the design and architecture that enables secure and transparent deployment of home and automotive digital twins. They can contribute to initiating and maintaining trusted relationships among individuals, insurance service providers, and public support providers. The paper also outlines a preliminary proof of concept of the framework tested with discussions facilitated by the insurance ecosystems envisioned within research and innovation programs.

5.1. Case Study 1: Implementing AI in Identity Verification

Technologies such as artificial intelligence, machine learning, and biometric solutions hold the potential for a new age of secure identity verification within the insurance industry. New technology allows businesses to collect more information about any individual than ever before and apply algorithms that provide new insights or actionable results from that data. By utilizing technologies that interrogate data, artificial intelligence agents are increasingly able to identify fraudulent behavior by analyzing patterns and creating profiles, monitoring threshold behavior, and building up large network information pools to inspect increased claims. In this paper, we examine how and where artificial intelligence can be most beneficial, focusing on the function of identity verification, which is at the heart of many insurance claims. In our model, we offer a framework that addresses identification fraud in the customer searching or claiming process. Agentic fraud claims supply literature to the business practitioner that describes the role individuals can play in top-level fraud in the process. We have examined the difficulty in operationally distinguishing between 'non-top-down' agentic fraud-causing behaviors such as carelessness, compared with the formal model of corruption within the organization or process of operation. By focusing on the potential causes of 'to trend down' fraud drivers, we examine how responsible and effective care labels can reduce the number of unreliable fraud narratives to the insurance company. Our model is then applied to a specific case where the framework has been proposed in an insurance ecosystem. We also demonstrate the application through several examples to understand the key elements and structures.

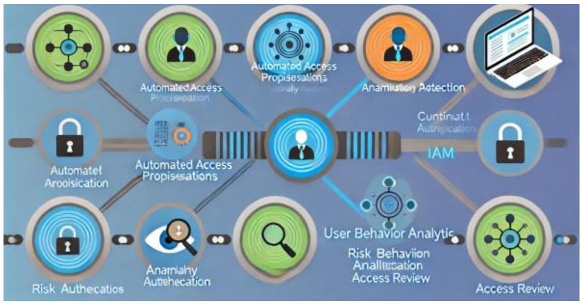

Fig 3 : AI in Identity and Access Management

5.2. Case Study 2: Access Control in Insurance Platforms

In this section, we consider a sample case study, ICARE: an insurance platform designed and implemented by a company. The structure, implementation, and operation of ICARE are protected by international patents. The company was a service company under a group, and the first insurance company was established in 2017. The family, in partnership with another family, expanded this platform over time. Another insurance and reinsurance company and a group of companies were established on this platform. The system integrated with ICARE operated as a backend for customers who were part of a leading retail chain tender and built customized insurance policies. Two medium- and low-income family insurance brokers joined the system and were also selling services. An adult training organization supported by investor insurance companies is included in the platform, and users of the platform are promoting training, with the purpose of training insurance policies.

Equation 2 : Trust Score Computation

$$T = \frac{\sum w_i S_i}{\sum w_i}$$

T = Trust score,

S_i = Security attributes,

w_i = Weight of each attribute.

5.3. Case Study 3: Incident Response and Mitigation

As an insurance partner, the department’s AI analyzed social media and identified several rumors that suddenly appeared on social media about a famous organization that faced a personal data leak caused by its failure of identity and access management systems. Following its real-time risk monitoring and management strategy, the insurance company knew that immediate damage control was crucial for the insured organization. An incident response and mitigation team was strategically assembled, and through the efforts of its cybersecurity and other task force members, the team quickly analyzed the relevant causes of the problem, offering a professional incident response and management service. Security experts from the domain and partners worked together to create a public relations statement and took other appropriate parts of the damage control ideology. The incident was defused, the causes were controlled immediately, and the company’s market was contained.

The incident investigation team reported that an external identity had been provided to ensure prompt updates were performed by using the services of the professional who currently was not working for the organization. The indicated list of triggers that were wrongfully granted some registered identity whose workflow access rights should be adjusted, resulting in an identity reaching critical levels because it was not immediately revoked when the employee stopped working with the organization. The auditing task appearing with regular systems found changes that should not have occurred within the constructs.

6. Technology Stack

Information technology (IT) tools and environment play a very important role in technology accelerating business. These digital support systems for business services enable insurance and reinsurance firms to perform their core businesses in a more efficient, effective, and productive manner. The technology stack in use implies cloud-first and mobile capabilities to maximally satisfy the evolving business digital ecosystem needs. This technology stack in use in this study consists of tools for data management, protection, processing, storage, and services for different categories of technology infrastructure within a given infrastructure environment. Supporting fabric technology enables the integration of intended target systems and systems promoting service-oriented architecture automation tools. The agentic AI-driven IAMF for SIsecOs is intended to enable the digital ecosystem service provider IT teams charged with the responsibility to build and operate secure insurance service ecosystems.

This responsibility is primarily focused on onboarding and enabling an organization’s end users, both clients and employees, by effectively provisioning access privileges for these end users when they require these services, with the right level of privileges for the period these services are required. The proposed framework demonstrates how AI technology services, delivered by different categories of workforce resources, augment the insurance service ecosystem’s foundational fabric properties with the agency as needed. It should be considered as far as the promotion, enablement, and practice of insurtech innovation is concerned. The technology stack takes advantage of market-proven strategic security and identity and access management solutions, some available as cloud services, others requiring that we work with mature, agile, capable vendors.

6.1. AI Technologies for IAM

Innovation in artificial intelligence (AI) technology has driven significant progress across sectors, including cybersecurity. A wide variety of tangible AI solutions in this specific domain has emerged, addressing several use cases, including adaptive authentication, anomaly detection and response, and AI offering conversational security in IAM. Traditional IAM capabilities are being augmented and, in many cases, made more effective by the use of AI. Less interactively, AI-powered automation and analytics can both reduce costs and improve cybersecurity. AI, without hands-on control, can mobilize many enterprise resources, automatically reconfigure network configurations, and automate incident response. By doing so, it is possible to greatly reduce the mean time to detect and the mean time to respond. In the area of anomaly detection and prediction, AI has also emerged as a powerful tool. AI-based anomaly detection uses machine learning techniques to model normal behavior and detect deviations from it. Such techniques are particularly useful for securing financial services.

6.2. Blockchain for Security

From a security perspective, blockchain technology has gained popularity for decentralized, secure, and immutable property. Blockchain can be leveraged for the implementation of secure identity and access management systems that manage individuals' identities and their access to intelligently control the security of the organization's resources. Blockchain technology can control, audit, and monitor access privileges from the root and change the way enterprises build access control by implementing it for identity and access management systems, whether it is for internal use or use in inter-organizational collaborative environments. Blockchain technology is a common decentralized storage system with immutable transaction records that has an amazing potential to provide data security for service transactions. This increased interest in creating user-centric models for privacy and data security in the domain of blockchain technology that sustains service transactions is making strides in the formation of technical spaces.

As long as the rules are followed, blockchain will honor the value of consent, take measures to treat personal information in digital form as individuals intend, and verify the identity and authority of data. These features inevitably suggest a promising blockchain structure in the form of a preliminary privacy-preserving concept for the assurance of service transactions. Specifically, global access to health records cannot be hacked or compromised, as well as the construction of simulated medical histories by accessing hospital service policies. A professional entity needs to overcome concerns about hacking, data manipulation, or structural shortcomings in existing health data management. The proposed mechanism has real social value: decentralized management is expedited and convenient through the use of strategic data sharing, and through blockchain technology, data authorization and verification of professionalism are advanced, while subsequent data release is improved, ensuring data security. Furthermore, the proposed framework is specifically implemented in health resource applications, with the ability to support other cross-sector services in the blockchain industry.

6.3. Cloud Solutions for Scalability

Cloud deployment models such as software as a service, infrastructure as a service, and platform as a service can be leveraged to support the scalability of the proposed agentive AI analytics component. Cloud-based deployment architecture is practically useful in making the resources more scalable and accessible. Cloud resources provide the advantage of highly scalable and elastic business services, such as network, storage, and virtual machine management, while releasing stakeholders from the complexities of fine-grained interactions that arise from the nature of these resources. Thus, cloud resources support agility, resource elasticity, and horizontal scalability, which are relevant for handling and processing big data economically and efficiently. These capabilities are particularly useful for big data use cases, from the development, testing, and integration of the analytics data pipeline to the analysis, visualization, and exploitation of the results. The developed cloud-based secure AI analytics platform can also be used to support future expansion into other domains, where hyper-automation, data-driven digital twins, or personal assistants may need to be utilized.

The distinction between on-premise architecture and cloud architecture is becoming even more unclear as companies may procure resources from the cloud and maintain sophisticated data centers, covering specific workloads on-premise. Common patterns for hybrid architectures are mainly based on geographical criteria. This shift has implications for the evolution of the cloud white-box business model. While on-premise customers will evolve into hybrid ones, cloud providers will face an increasing demand for solutions addressing hybrid architectures. Because of the split between on-premise and cloud architectures, products for data analysis need to provide scalable and on-premise deployable solutions. Segregation, data privacy, and the rise of multi-architecture solutions are not just byproducts but are desired features of AI solutions in the upcoming era. Market trends indeed support an increasing demand for AI-driven solutions that can process information close to the sources where it is generated, such as healthcare, industrial, or highly sensitive scenarios. We are thus facing a significant transformation in the distributed computing landscape, and the offered solution cannot ignore that the future of artificial intelligence-driven analytics should fully support these scenarios. Data can be either generated, processed, or reside in a location. The classical simplistic computing concept cannot be confirmed; the decision on where to execute a complex machine learning model cannot be taken lightly based on performance criteria exclusively. We applied our platform to solve real business cases for insurers, who take advantage of the evolutive and flexible AI-driven models we provided to address emerging needs. The implications can be traced back to the need to offer hybrid solutions, where specific models are tailored for different deployment environments and can perform transfer learning by providing model bootstrapping.

7. Regulatory Considerations

In recent years, there seems to be an occasion for consumers in Indonesia to have insurance, especially with the socialization of insurance by government-supported campaigns, as well as the realization of progress towards achieving the insurance penetration level. With the increasing number of insurance consumers in Indonesia, it is expected that the AI-driven identity and access management framework that has been offered will reduce the phenomenon of user fatigue while also benefiting the insurance companies acting as identity providers. This is in line with Indonesia's Presidential Regulation concerning Indonesia's National Strategy for the Digital Economy. One of the strategies of the digital economy is the reduction of user fatigue. The Ministry of Transportation Directives for Road Safety also encourages research related to insurance that can assist in the process of reducing user fatigue. Meanwhile, the terms and conditions of the insurance apply to a contract. The insurance company is responsible for providing information about the contract and ensuring that the information can be easily understood by the consumer. This regulation also supports the results of AI-driven identity and access management in the form of business opportunities that have been opened by consumers in the insurance industry and creates value for insurance services by noticing consumer identity behavior. The results of this research are more significant when the application of identity and access in the insurance business is easy for the user and the insurance company itself.

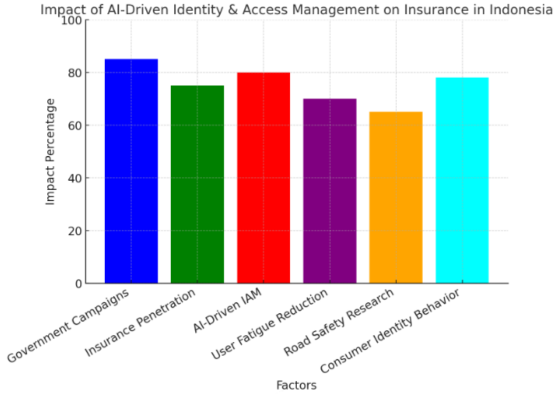

Fig 4 : AI-Driven Identity & Access Management in Indonesia's Insurance Sector

7.1. Data Protection Regulations

The right to privacy is a fundamental human right recognized globally by most constitutions and legal frameworks. It is a right that is increasingly sought to be abridged in a digital-first world for systems and services that are accessed through digital mediums. This is achieved through the repurposing of personal data collected to refine customer experience and build user models for targeted offerings. This became a problem when the frameworks that regulated information privacy were soon outpaced by technological innovation. This lack of privacy regulation allowed various rights granted by legislation to be diluted or subverted by private technology companies for commercial purposes, leading to privacy diversions that resulted in national security risks and fostering uncertain relationships between nations. This manifested in data renegotiation battles and international forums for technology companies and nations alike, conduct that did not help any regulatory body to advance an international norm that would advance democratic principles globally, forcing nations to take unilateral measures to address these concerns.

As the digital environment continues to grow rapidly, the European Union initiated a strategy with the main aim being to provide individuals with the ability to exercise control over their data. This strategy has come to be known as the General Data Protection Regulation, and it requires global organizations to comply with its regulations but does not create any forum through which non-EU member countries can become active participants in the same. Efforts had been initiated to come up with similar regulatory frameworks in the United States, but such strategies were never fully embraced. The single regulatory space leading to a data mesh was never built, resulting in a global privacy landscape that was extremely fragmented. To address privacy concerns, companies started creating internal security policies that required the implementation of data protection policies that limited access to personal and sensitive data. This minimized the visibility that the organization's technical teams had when resolving complex application issues, which in turn compromised the top priorities of efficient time, cost, service reliability, and customer satisfaction, which drove them to divert from secure policies for data management. This resulted in non-compliance with data privacy regulations being added to the security budgets of organizations, as recent survey data revealed, a number that seems to increase with each wave openly voicing the loss of brand reputation, user trust, customer satisfaction, and revenue due to data breaches. Although these issues are important for all industries, they are particularly important to highly regulated verticals like the insurance industry. Some of the reasons why the data protection and privacy problem is important to this industry are due to the mass of personal and business data that falls under the purview of business operations that are necessary on a global scale to support customers, where the existing technology does not support the many levels of automation necessary to provide flexibility and service quality improvements in a manner that data privacy concerns are addressed. The importance of implementing this kind of technology has never been more pronounced, especially as operational disruption can cause a company to lose its competitive edge in the insurance spectrum. High-profile data breaches and privacy issues on globally recognized identities are some of the reasons why the insurance industry is a common feature in lists of organizations with data privacy issues amounting to millions of dollars. Finally, the insurance industry is vulnerable to attacks and cybersecurity risks due to the threat posed by rogue agents and malicious or accidental agents who are unwilling or unable to follow established channel security best practices to access data and then repurpose these data sets.

7.2. Compliance in Insurance Sector

The governments of several countries globally are imposing newer and stricter regulatory guidelines for most industries. This includes BFSI, which is targeted to offer enhanced data privacy and protection for consumers. In several countries, the data privacy acts are continuously updated with innovative and highly structured surveillance programs, empowered by artificial intelligence and big data. Organizations need to abide by these regulations and ensure compliance while dealing with sensitive consumer data. Training AI platforms that prioritize data protection will not only help manage the increased data protection risks imposed by the restrictions but also leverage these data protection tools to ascertain the success of the actors in the long term. The existing administration of data protection legal principles and rules is becoming more sophisticated and complicated. These systems assist companies in better managing their incident data. Tools including consent and contract administration systems that provide ways to generate, maintain, and restore consumer agreements and commercial documents would become an important aspect of reaching and maintaining adherence in various applications of software used to address personal data.

Not just the insurance companies, but the insurtech and crypto insurance companies also have to maintain compliance with these laws. To better accomplish the success of the straightforwardly low-regulation finance pledge, a combination of standard fund services coupled with a selection of basic investment policy and procedural ratios, internal supervisory checks, and external positions and asset transformations and control operations should be implemented. Maintaining advanced and corporate policy support processes would be crucial for preventing a company from falling behind its contingencies. A large volume of groundwork is required to guarantee the smooth running and continuity of workflows. Such tasks would need to be undertaken with the help of tools. Conventional approaches can struggle to offer these services, and up-to-date technologies such as process and jurisdiction analytics, enhancing processing outputs with the help of artificial intelligence algorithms and blockchain record-keeping can help accelerate most activities that were completed before. To rise to the demand for advanced and up-and-coming policy support solutions, the software is supposed to become superior in virtually every case. Software solutions should offer proven ways so that a firm can be sure that these systems would be fed the right signals and controlled through artificial intelligence capabilities. As a consequence, the software is evolving into a complex AI-based monitoring solution that adjusts to the specific contexts and settings of an employment scenario, ultimately providing consistent, accurate, and practical business input.

7.3. Ethical Considerations of AI

With the even more significant role that AI is playing in terms of achieving positive ethical situations, it is valid to scrutinize to what extent the systems created in the AI field could affect business applications and various industries in protecting ethical activities. Especially, the level of AI with agentic capabilities is a separate status with rules, and there are serious actions in particular: How will an AI agent be accountable to all? Who would take a robot to court? AI-agnostic capabilities should therefore not be of what level or type, at least to avoid unnecessary ethical issues and to delay litigation. The ethical requirements for any level of AI, especially how to be incorporated or implemented into agentic AI, are disputed and widely defined. One could then decide which AI is required in any industry to pursue an ethical approach and plan to create that AI system in the approach to creating an AI application. As mentioned earlier, any undertaking or entity that deals with AI should embrace ethics as a major facet, and it could be proven to be an asset, so consider it worth the confidence capitalization.

In member states, the EU has already committed to becoming a leading trust partner in AI and the development of strategies and voluntary codes of conduct on AI. A draft Code of Ethics appears to be one of the first formal measures taken by the President’s office to guarantee that its public services use AI and autonomous technology responsibly and ethically. In particular, it is stated that ethics should be at the core of AI in a significant number of AI-related high-level activities, strategies, and reports. In addition to the report, a recent international professional conference has been organized in an attempt to mount the advantages of accelerating the ethical and inclusive operation of AI. The insurance industry should also formulate a list of ethical priorities and follow a nominal commitment not only to build or embrace AI but to incorporate ethical AI.

8. Implementation Strategies

A good implementation plan would prioritize the AI integration, toolkit selection, and development activity areas and technologies identified in the proposed AI-Driven Identity and Access Management framework. The insurance and AI commerce taxonomy models would be used as a reference while implementing the commerce-sided AI characteristics. This taxonomy could be considered a trade-off in the economic trade-off, as its implementation will affect costs and customer experience. As with the adoption of any AI technology, it is important to proceed with an understanding of organizational readiness. The innovative market and technology characteristics that include the four technology readiness characteristics and the five insurance market segments help organizations understand the impact of technology on the potential success of the AI-IAM framework. Another implementation strategy would be adapting the composed architecture for key sectors like healthcare and finance outside the insurance industry. The tested AI-IAM model and the framework of the insurance case would be adapted to these sectors with sufficient depth to build a use case. This research proposes a viable solution for IAM in businesses using AI. An AI model that is used for solution composition and decision-making is sufficient as a proof of concept. The implemented model is easily adaptable to vast application areas. Building TACIAM-MV, an AI with a large-scale commercial existing system, would disrupt the IAM scenario. This disruption is followed by other main systems and would require a top-down, painful change management strategy. Further, this approach is easily adaptable to vital systems, including complete security coverage of large-scale networks for government, commercial ventures, and vertical sectors. It is essential to shift business systems toward AI as a top IT priority, especially with the current automation trend across industry sectors. Sparkling IAM is a starting 'killer' application in the present digital transformation era. Information security covers large-scale AI-driven systems. Organizations are highly encouraged to use the proposed AI-driven IAM architecture to decrease risks in critical primary systems, bringing business transformation.

8.1. Phased Rollout Approach

Trying to roll out any complex system such as the proposed framework all at once, either in testing or production environments, puts an unnecessary level of risk to both the organization and the projects. It is imperative to have a phased approach that allows organizations to have early visibility into what is being developed and tested and to use those results to refine both the framework as well as achievable expectations of the organization for the remainder of the framework rollout. It also gets end users and application teams familiar with the technology and the portal, which increases their comfort as the technology is rolled out to additional resources. Finally, it creates several smaller, manageable projects rather than one large, hard-to-manage project.

In an insurance ecosystem or a given product line, one might see all of the following resources as they relate to the products that are being developed in a concurrent environment: contact information, the insurance contracts, the formal definition of the various data elements that the insurance contracts rely on, premium payment transactions and contacts, company employees, the applications, and the code that they run, etc. If all of these resource types and others are to be linked using the proposed approach, likely phase 1 of the rollout will occur at the UI level and will present several editing widgets that have been developed across all of the insurance contracts, contract attributes, and company employee types in that it interacts. The UI widget is being tested by the applications that use it, with UI applications ranging from simple testing to fully deployed service calls. However, the UI widget is the only code deployed. Starting with this small but useful aspect of the overall framework, the organization will see real benefits associated with using the framework in phase 1.

8.2. Training and Change Management

Successful project implementation purely depends on the success of employees' adaptations to the systems and solutions that are to be implemented. Often, in many organizations, people are the most affected by change and are the easy targets for resistance to change—directly threatening implementation and, consequently, the success of change. Employees throughout the entire organization undergo direct or indirect impact through change. To ensure efficient adjustment to the change, it is essential to have in place, and to implement, efficient programs to address training and change management, along with broader organizational interventions. This is even more relevant and valid for organizations that are transformation-focused or are embracing advanced digital or AI technologies, which are slowly transforming their business interactions with clients.

After many years of observation, it has become clear that management must undertake measures to assist and stimulate staff to adapt to change. No change will be successful without some level of training, regardless of the focus being on training either the staff or their management. Successful transitions do not just happen. Organizational design benefits from building proactive activities that support transitions. Such practices minimize disruption and can enhance transitions. It is therefore imperative that insurance industry stakeholders prioritize ongoing employee engagement and training to optimize transparency, maintain engagement, capture value from change programs, and develop management capabilities in the long term. Successful change management leads to enhanced business processes and success. Confidence and proactive involvement ensure improvements that leverage the full strength of the workforce.

Employees who feel engaged actively participate and fully commit themselves to the activities of the organization. Such employees show creativity and innovation. As a part of their adaptability to change, they demonstrate flexibility in a dynamic environment and accept the need to learn new skills. Every employee involved in day-to-day work has a wealth of knowledge about business operations. Employees are, in many cases, the best source of information about an organization's policies, procedures, and processes. It becomes essential that they fully understand their role and responsibility within change initiatives to better recognize the value of their involvement.

8.3. Monitoring and Evaluation

The process of preventive prediction at the initial phases is tightly integrated with the identity and access management control policies and occurs before insiders' intentions become clear. It creates a feedback loop where the system's consequences are monitored and considered when IAM policies are defined or adjusted. This change in focus on the targeted area for attack leads to a dynamic environment where the protective measures adapt to the environment under the initialization of the threat. Furthermore, acting in a fast-changing, intricate, adversarial cyber environment, access management must meet a bevy of goals to be truly effective. The most important goals we achieved are to facilitate the needed access without excessive limitations while ensuring that all activity is by enterprise policies and also to enforce that everyone else has only the access necessary to perform their job.

The detection and prediction models employed in our sensed IAM process need to be continuously and iteratively developed. Prioritized insider threat early detection represents a significant concern and requires the systematic organization of all involved for its solution. We manifest the importance of explicitly investing effort and resources to come to the inception stage of a complex problem to increase our likelihood of prevailing during the execution stage. Unlike in discussions of evidence-based managerial innovations where the paperwork seems unfeasibly overwhelming due to the manager's severe time and resource constraints, insider threat early detection indeed conveys crucial and decisive importance, and reasonable continuing effort is by necessity redirected towards its assurance. These factors weigh in favor of the presentation of another detailed proposal ensemble for prioritized insider threat early detection, which proposes and addresses new and pressing issues related to the merging, assessment, retargeting, and upkeep of evolving, dynamic, early detection, and escape models.

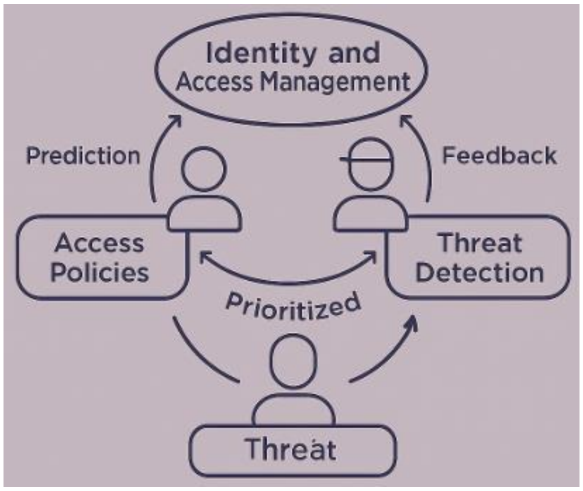

Fig 5 : Insider Threat Early Detection

9. Challenges and Limitations

Leveraging the various capabilities of AI in IAM also brings a lot of challenges and limitations. AI-based IAM processes require a massive amount of historical data from all participants in the insurance ecosystem for accurate behavior analysis and prediction. As AI can directly impact identity access privileges, access management, or IAM, its ability to consistently control AI behavioral outputs is very critical. AI models can be easily spoofed when dealing with large amounts of data by deliberately perturbing predictable input. When machine learning models, including deep learning, receive data that appear with normal perturbations to a human observer, they could behave abnormally. A single compromised point of focus can enable attackers to leverage AI capabilities for mass damage. Whilst these offerings from AI in IAM process designers and developers in insurance ecosystems, they should always understand and assess the selection, performance, and security of AI models and the governance elements brought by AI concepts such as model and decision explainability. AI models for identity access privileges need to be built to achieve a balance between performance and algorithmic fairness. They should also be trained and operated in the right ethical framework to ensure that any bias from data, human review, or training is minimized.

9.1. Technical Challenges

The envisioned Agentic AI-driven IAM framework faces several technical challenges. The paradigm essentially transforms users and devices into agents, and IT and OT systems into agent societies. These communities, with millions of user and device agents and a large social network, must be modeled and reasoned effectively to provide secure access control services. This likely involves cloud-based account management and naming services, and domain-specific group and role management services. Names and roles must be lightweight to not create a heavy burden on agents. Existing trust anchors could overlay the agents with a trust fabric and enable the agent groupings.
The second concern is to provide agents that can interface with a wide variety of users and devices and enforce access control policies effectively. This would involve some neural-like intelligence to detect and interpret inputs, sense the user experience, and interface with users and devices to handle access control policy effectively, particularly when understanding natural language.
The third concern is to provide agent communities that leverage both human security knowledge and proven and verified machine security knowledge. Identity verification processes are normally carried out by humans who rely on their knowledge, experience, and available knowledge bases to make decisions. Skilled security experts, particularly in the organization and management of PII types, can also be considered agents. Such as data controllers, and authorization managers who keep records of any authorized transactions to make all members responsible for operating a registry on transaction-level codes, ensuring data is managed safely. Compliance managers report to DPAs any violations of the internal rules of the data reviewing mechanism. Grouping agents to enforce data protection principles.

9.2. User Adoption Issues

The agentic success model stresses the vital role of the individual user in successful system acceptance and use. Personal acceptance is a crucial aspect of IT adoption. Emotional attachment and a positive relationship between the individual and an effective agent of the information system may serve to significantly improve the person’s acceptance of the system. In learning organization literature, agents or champions play important roles in facilitating knowledge management adoption as well as activities. In other IT systems, such user agents are known as "change agents," "technology champions," or "IS leaders." Knowledge management success is the creation and absorption of new knowledge through change agents. The impact can be likened to a multiplier effect that raises benefits such as customer satisfaction, profitability, and market share by producing cascading positive effects that start with adoption. The creation and use of guidelines that specify the responsibilities, level of authority, required skills, and necessary resources, especially time needed, for the knowledge management agent during the knowledge management process can help increase the chances of successful changes and build the level of trust between the agent and team members.
This chapter proposes a novel framework to help insurance technology professionals understand how to create AI-driven Identity as a Service (IDaaS) that is worthy of the

promise of ease of use. They should leverage AI to actively convert digital identities and learn how to become AI-driven agents of such a platform by observing user behavior patterns. With the advent of AI, dynamics have changed what is possible. AI can learn employees' behavior along with the parameters of ease for consumers, so practitioners no longer have to ask all users to adapt to the platform's way of doing things; they can instead create a smart platform that functions within models to learn the way each user in the diverse community of stakeholders does things and accordingly personalizes the experience in a way that feels easy. In sum, ideally, stakeholders should invest in AI that is valuable in driving products toward ease of use and observed engagements.

9.3. Regulatory Hurdles

This research emphasizes the urgent need for regulatory authorities, concerned stakeholders, and AI and fintech panels to collaborate in resolving the serious regulatory, auditing, assessment, and oversight challenges. By following ethical, practical, and lawful AI governance frameworks, the synergies between AI and security advancements should be taken into account and employed by the whole insurance industry, including insurance and digital insurance disruptors. The global insurance industry should cease to ignore, de-prioritize, or misunderstand the serious advantages of state-of-the-art AI-automatable cybersecurity, learn the practical lessons from similar studies, and, finally, undertake cybersecurity-centric AI-driven innovations in earnest.

The next critical step is the extensive global cooperation led by the concerned stakeholders in establishing and adopting AI cybersecurity frameworks for existing and upcoming insurance. This dialogue should explore the migration trajectories of insurance allowabilities, highlighting them as necessary for practical and lawful AI deployments in cybersecurity and insurance. The upcoming AI and cybersecurity community, insurance and insurance association events, working group task forces, industry studies, and special AI, cybersecurity, and insurance conference tracks should focus on AI do's, rather than the social impact of AI don'ts, which have destroyed the AI market potential in loads of the same old, standard AI solutions problems.

10. Future Directions

Currently, our AI-driven IAI framework provides an understanding of how user identities could be utilized to enable secure operations for insurance services within an InsE. Therefore, the next step would be to provide enhancements in this regard. We focus on the integration of IAM as a service into our AI-driven IAI framework. Making IAM services programmatically accessible allows it to be delivered as a function of the "stack" that developers or within integration workloads. The latter not only builds the functionality into a larger service or application but also utilizes the API to deliver the service chronically. The IAM "as-a-Service" could then be offered through cloud service providers or as a cloud-native service being offered privately or commercially.

Analyzing identity and access management operations is extremely important to determine when there are violations of policy, misuse, or inappropriate authorization of an identity. It also establishes a foundation of confidence by verifying that identities are performing intended activities by security policy. About AI, several automated methods could put the transformational power of the technology to work on the IAM problem. As with any protection domain, policies are created to secure access to resources based on authentication and authorization techniques. The IAM process checks user requirements and grants corresponding authorizations, which can utilize AI algorithms to observe access requests and infer patterns of behavior that establish a profiling baseline specific to the entity. From this newly developed perspective, we ask identity and access management frameworks to reshape solutions such that degrees of 'trusted' identity and 'trusted' access are evaluated with a higher degree of certainty.

10.1. Advancements in AI for IAM

AI has evolved significantly through the technique of deep learning in the last decade and has been deployed successfully in real-world applications. However, large-scale deployment has been fraught with extensive preparation of data, longer training times, limited robustness, and expensive hardware requirements. These restrictions are being addressed by using explainable AI and human-augmented AI approaches, biased dataset cleansing, and quicker adversarial training data generation through machine learning to reduce the threat of adversarial poisoning. These measures are necessary for the application of AI for IAM, which is the goal of this work. The application areas of AI for IAM include reducing false positives and false negatives in a tip-off and scene analysis of video surveillance, shutdown and surveillance on finding cheaters, invisible privacy through face de-identifications in-vehicle surveillance video, and effective identity range search in large-scale face databases.

With the increasing parameter count and network complexity of deep neural networks, the decision-making process of these networks becomes less transparent. This has led to a growing interest in enforcing explainability on their outputs. Despite numerous appealing characteristics, deep neural networks are sensitive to adversarial perturbations, potentially causing catastrophic damage in critical applications, of which intelligent surveillance is an important category. Detection of these adversarial inputs, though of utmost importance, involves additional steps during training and testing and often incurs significant computational overhead. Recent studies also suggest the existence of a widespread adversarial structure that can render adversarial attacks extremely easy on most in-the-wild data, decreasing the practicality of deep neural networks. This 'adversarial susceptibility' inspires us to rethink our approaches to intelligent surveillance.

10.2. Potential for Decentralized Identity Solutions

Insurance ecosystems span across many industry verticals to serve various individual, household, and business risks and financial needs. Securing the confidence and trust of all the ecosystem participants is of paramount importance to better serve customers, reduce losses, increase profitability, and satisfy regulatory requirements. Identity and access management systems play a critical role in ensuring security and privacy interests while enabling real-time collaboration and access. However, current IAM models are centralistic and do not give the necessary control and power to the individual subjects with the desired level of autonomy and data protection. Future-proof insurance ecosystems that can effectively anticipate and manage upcoming trends and challenges need decentralized IAM models that can provide different aspects of control, security, and privacy to individuals. While having the necessary features, decentralized IAM solutions could elegantly establish a fine balance between the various security requirements and the value creation of the ecosystem. These requirements, coupled with the number of only loosely coordinated participants, the positive implications of making digital ecosystems and digital transactions safer, and the altruistic social impact mission of the insurance industry, increase the potential for self-sovereign and decentralized identity solutions to fundamentally transform the industry.

Equation 3 : Anomaly Detection in Access Requests

$$D = \sum |X_i - \mu|$$

D = Deviation score,

X_i = Access request feature,

μ = Expected behavior.

10.3. Long-term Vision for Secure Insurance Ecosystems

Looking towards the future, there will be much research for the creation of a secure insurance ecosystem powered by human-AI mentorship with sensible and agentic AI driven by smart, human-initiated, and smart, human-managed friction. The proposed framework is a nascent step forward in beginning this conceptual journey. Human-operated ecosystems with AI mentorship provide innovative avenues for insurance ecosystems to be both agile and secure in equal proportions. Computer security has always been, and will always be an innovation problem. This innovative problem cannot be solved by technology alone, because artificial intelligence will always be inferior to human cognition. Our vision for 2031 is to envision a world of innovative, secure, and human-empowered insurance ecosystems without technical complexity, bureaucracy, and didactic governance that rules within strict controls and divides us. In the digital tide of fashion from fear and chaos to controlled absolutism, the framework places itself in the uncomfortable but influential middle area.

It has been acknowledged, again and again, that trust (between organizations, between systems) must be there for our digital existence as individuals, employees, customers, and citizens of the Internet. We trust technical systems (and concentrate on the development of this trust), and we trust organizations (we are always blaming the processes for our potential infallibility), but the faith or distrust of the people who drive trusted technical systems and trusted organizations seems to have been blinded or rooted out as a potential factor facilitating the easy introduction of innovations that might act as an equal (but indispensable) remedy for fears of relating to and secure digital sharing. By 2031, try to uplift trust in the future, at least towards broader innovative and constructive applications, such as original insurance information and guidance. Our agentic framework represents one of the ways to initiate flexible, self-governing insurance ecosystems with AI from human mentorship that maintain current levels of cybersecurity while appropriate new levels of secure digital proactivity are explored.

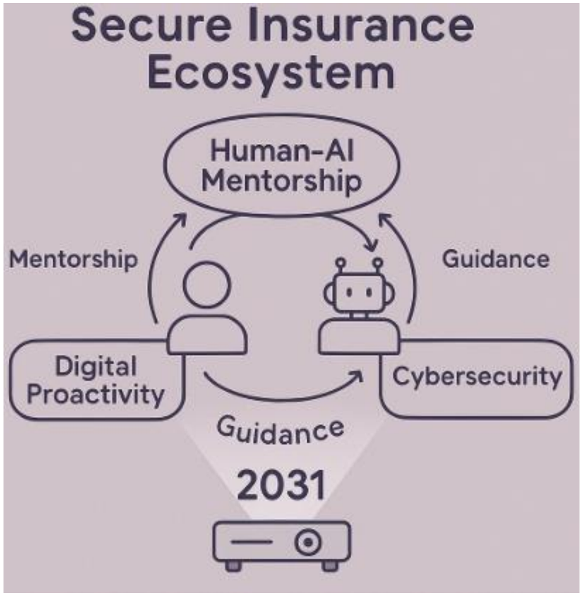

Fig 6 : Long-term Vision for Secure Insurance Ecosystems

11. Conclusion

This paper has presented an agent-relayed token management framework for managing digital identities in insurance ecosystems. The proposed framework uses a token schema comprising the agent, receiver realm, sender realm, and several attributes to construct tokens with minimal levels of disclosure subject to the requirements of the receiver's security policy. The token management framework connects several interacting agents to construct and issue tokens within an organization and across insurance business partners. The salient feature of the proposed work is that it takes into account existing relationships between the sender, receiver, and the agent issuing tokens.

The agent relayed token management framework along with the end-to-end approach presented provides an excellent culture to enable the insurance industry to introduce the appropriate IAM capable of an ecosystem approach. It also enables the use of AI and ML capabilities to learn, predict, and remediate breaches, further strengthening organizational security. The proposed framework offers the flexibility of decentralizing the IAM by supporting customer adds, modifies, and manages profiles in legacy and cloud environments, thus paving the way for a truly effective agent-agnostic, and self-service paradigm. Since our framework also constructs a minimal token with minimal attribute values, it paves the way for pseudo-anonymous and anonymous insurance transactions in an insurance blockchain.

12. References

[1] Lakshminarayana Reddy Kothapalli Sondinti, Ravi Kumar Vankayalapati, Shakir Syed, Ramanakar Reddy Danda, Rama Chandra Rao Nampalli, Kiran Kumar Maguluri, & Yasmeen. (2024). Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth. The Bioscan, 19(Special Issue-1), 639–645. https://doi.org/10.63001/tbs.2024.v19.i02.S.I(1).pp639-645

[2] Burugulla, J. K. R. (2024). The Future of Digital Financial Security: Integrating AI, Cloud, and Big Data for Fraud Prevention and Real Time Transaction Monitoring in Payment Systems. MSW Management Journal, 34(2), 711-730.

[3] Annapareddy, V. N., & Sudha Rani, P. (2024). AI and ML Applications in RealTime Energy Monitoring and Optimization for Residential Solar Power Systems. Available at SSRN 5116062.

[4] Polineni, T. N. S., Ganti, V. K. A. T., Maguluri, K. K., & Rani, P. S. (2024). AI-Driven Analysis of Lifestyle Patterns for Early Detection of Metabolic Disorders. Journal of Computational Analysis and Applications, 33(8).

[5] Venkata Bhardwaj Komaragiri. (2024). Generative AI-Powered Service Operating Systems: A Comprehensive Study of Neural Network Applications for Intelligent Data Management and Service Optimization . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 1841–1856. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1861

[6] Vamsee Pamisetty. (2024). AI Powered Decision Support Systems in Government Financial Management: Transforming Policy Implementation and Fiscal Responsibility. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 1910–1925. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1928

[7] Polineni, T. N. S. (2024). Integrating Quantum Computing and Big Data Analytics for Accelerated Drug Discovery: A New Paradigm in Healthcare Innovation. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 38-49.

[8] Paleti, S. Agentic AI in Financial Decision-Making: Enhancing Customer Risk Profiling, Predictive Loan Approvals, and Automated Treasury Management in Modern Banking.

[9] Challa, S. R. Behavioral Finance in Financial Advisory Services: Analyzing Investor DecisionMaking and Risk Management in Wealth Accumulation.

[10] Shyamala Anto Mary, P., Kalisetty, S., & Mandala, V. M. (2024). Advancing IoT Data

Forecasting with Deep Learning Framework for Resilience Scalability and Real-World Applications. Srinivas and C, Chethana and B, Thevahi and Mandala, Vishwanadham and M, Balaji, Advancing IoT Data Forecasting with Deep Learning Framework for Resilience Scalability and Real-World Applications (November 15, 2024).

[11] Kannan, S., & Seenu, A. (2024). Advancing Sustainability Goals with AI Neural Networks: A Study on Machine Learning Integration for Resource Optimization and Environmental Impact Reduction. management, 32(2).

[12] Sambasiva Rao Suura (2024) Generative AI Frameworks for Precision Carrier Screening: Transforming Genetic Testing in Reproductive Health. Frontiers in Health Informa 4050-4069

[13] Nuka, S. T. (2024). Exploring AI and Generative AI in Healthcare Reimbursement Policies: Challenges, Ethical Considerations, and Future Innovations. International Journal of Medical Toxicology and Legal Medicine, 27(5), 574-584.

[14] Pallav Kumar Kaulwar. (2023). Tax Optimization and Compliance in Global Business Operations: Analyzing the Challenges and Opportunities of International Taxation Policies and Transfer Pricing. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 150-181. https://ijfin.com/index.php/ijfn/article/view/IJFIN_36_06_008

[15] Malempati, M., & Rani, P. S. Autonomous AI Ecosystems for Seamless Digital Transactions: Exploring Neural Network-Enhanced Predictive Payment Models.

[16] Sondinti, K., & Reddy, L. (2024). Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth. Financial Optimization in the Automotive Industry: Leveraging Cloud-Driven Big Data and AI for Cost Reduction and Revenue Growth (December 17, 2024).

[17] Challa, K. (2024). Neural Networks in Inclusive Financial Systems: Generative AI for Bridging the Gap Between Technology and Socioeconomic Equity. MSW Management Journal, 34(2), 749-763.

[18] Ramanakar Reddy Danda, Z. Y., Mandala, G., & Maguluri, K. K. Smart Medicine: The Role of Artificial Intelligence and Machine Learning in Next-Generation Healthcare Innovation.

[19] Karthik Chava, Kanthety Sundeep Saradhi. (2024). Emerging Applications of Generative AI and Deep Neural Networks in Modern Pharmaceutical Supply Chains: A Focus on Automated Insights and Decision-Making. South Eastern European Journal of Public Health, 20–45. https://doi.org/10.70135/seejph.vi.4441

[20] Sriram, H. K. (2023). Harnessing AI Neural Networks and Generative AI for Advanced Customer Engagement: Insights into Loyalty Programs, Marketing Automation, and Real-Time Analytics. Educational Administration: Theory and Practice, 29(4), 4361-4374.

[21] AI-Powered Revenue Management and Monetization: A Data Engineering Framework for Scalable Billing Systems in the Digital Economy . (2024). MSW Management Journal, 34(2), 776-787.

[22] Krishna AzithTejaGanti, V., Senthilkumar, K. P., Robinson L, T., Karunakaran, S., Pandugula, C., & Khatana, K. (2024). Energy-Efficient Real-Time Hybrid Deep Learning Framework for Adaptive Iot Intrusion Detection with Scalable and Dynamic Threat Mitigation. KP and Robinson L, Thomas and Karunakaran, S. and Pandugula, Chandrashekar and Khatana, Kavita, Energy-Efficient Real-Time Hybrid Deep Learning Framework for Adaptive Iot Intrusion Detection with Scalable and Dynamic Threat Mitigation (November 15, 2024).

[23] Chaitran Chakilam, Dr. P.R. Sudha Rani. (2024). Designing AI-Powered Neural Networks for Real-Time Insurance Benefit Analysis and Financial Assistance Optimization in Healthcare Services. South Eastern European

Journal of Public Health, 974–993. https://doi.org/10.70135/seejph.vi.4603

[24] Nampalli, R. C. R., & Adusupalli, B. (2024). Using Machine Learning for Predictive Freight Demand and Route Optimization in Road and Rail Logistics. Library of Progress-Library Science, Information Technology & Computer, 44(3).

[25] Intelligent Supply Chain Optimization: AI Driven Data Synchronization and Decision Making for Modern Logistics. (2024). MSW Management Journal, 34(2), 804-817.

[26] Syed, S., Jayalakshmi, S., Kumar Vankayalapati, R., Mandala, G., Yadav, O. P., & Yadav, A. K. (2024). A Robust and Scalable Deep Learning Framework for Real-Time Iot Intrusion Detection with Adaptive Energy Efficiency and Adversarial Resilience. Available at SSRN 5077791.

[27] R. Daruvuri, K. Patibandla, and P. Mannem, "Leveraging unsupervised learning for workload balancing and resource utilization in cloud architectures," International Research Journal of Modernization in Engineering Technology and Science, vol. 6, no. 10, pp. 1776-1784, 2024.

[28] Avinash Pamisetty. (2022). Enhancing Cloudnative Applications WITH Ai AND Ml: A Multicloud Strategy FOR Secure AND Scalable Business Operations. Migration Letters, 19(6), 1268–1284. Retrieved from https://migrationletters.com/index.php/ml/article/view/11696

[28] Somepalli, S. (2021). Dynamic Pricing and its Impact on the Utility Industry: Adoption and Benefits. Zenodo. https://doi.org/10.5281/ZENODO.14933981

[29] Nampalli, R. C. R., & Adusupalli, B. (2024). AI-Driven Neural Networks for Real-Time Passenger Flow Optimization in High-Speed Rail Networks. Nanotechnology Perceptions, 334-348.

[30] Chaitran Chakilam, Dr. Aaluri Seenu, (2024) Transformative Applications of AI and ML in Personalized Treatment Pathways: Enhancing Rare Disease Support Through Advanced Neural Networks. Frontiers in Health Informa 4032-4049

[31] Maguluri, K. K., Pandugula, C., & Yasmeen, Z. (2024). Neural Network Approaches for Real-Time Detection of Cardiovascular Abnormalities.

[32] Koppolu, H. K. R. Deep Learning and Agentic AI for Automated Payment Fraud Detection: Enhancing Merchant Services Through Predictive Intelligence.

[33] Sriram, H. K. (2022). AI Neural Networks In Credit Risk Assessment: Redefining Consumer Credit Monitoring And Fraud Protection Through Generative AI Techniques. Migration Letters, 19(6), 1017-1032.

[34] P. Mannem, R. Daruvuri, and K. K. Patibandla, "Leveraging Supervised Learning in Cloud Architectures for Automated Repetitive Tasks.," International Journal of Innovative Research in Science,Engineering and Technology, vol. 13, no. 10, pp. 18127–18136, Oct. 2024, doi: 10.15680/ijirset.2024.1311004.

[35] Chava, K. (2022). Redefining Pharmaceutical Distribution With AI-Infused Neural Networks: Generative AI Applications In Predictive Compliance And Operational Efficiency. Migration Letters, 19, 1905-1917.

[36] Yasmeen, Z., Machi, S., Maguluri, K. K., Mandala, G., & Reddy, R. (2024). Transforming Patient Outcomes: Cutting-Edge Applications of AI and ML in Predictive Healthcare. Transforming Patient Outcomes: Cutting-Edge Applications of AI and ML in Predictive Healthcare SEEJPH, 25, S1.

[37] Kishore Challa. (2024). Artificial Intelligence and Generative Neural Systems: Creating Smarter Customer Support Models for Digital Financial Services . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 1828–1840. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/1860

[38] Danda, R. R., Nampalli, R. C. R., Sondinti, L. R. K., Vankayalapati, R. K., Syed, S., Maguluri, K. K., & Yasmeen, Z. (2024). Harnessing Big Data and AI in Cloud-Powered Financial Decision-Making for Automotive and Healthcare Industries: A Comparative Analysis of Risk Management and Profit Optimization.

[39] Malempati, M. (2022). Machine Learning and Generative Neural Networks in Adaptive Risk Management: Pioneering Secure Financial Frameworks. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3718.

[40] Pallav Kumar Kaulwar. (2022). The Role of Digital Transformation in Financial Audit and Assurance: Leveraging AI and Blockchain for Enhanced Transparency and Accuracy. Mathematical Statistician and Engineering Applications, 71(4), 16679–16695. Retrieved from https://philstat.org/index.php/MSEA/article/view/2959

[41] Nuka, S. T. (2024). The Future of AI Enabled Medical Device Engineering: Integrating Predictive Analytics, Regulatory Automation, and Intelligent Manufacturing. MSW Management Journal, 34(2), 731-748.

[42] Sambasiva Rao Suura. (2024). Artificial Intelligence and Machine Learning in Genomic Medicine: Redefining the Future of Precision Diagnostics. South Eastern European Journal of Public Health, 955–973. https://doi.org/10.70135/seejph.vi.4602

[43] Kannan, S. The Convergence of AI, Machine Learning, and Neural Networks in Precision Agriculture: Generative AI as a Catalyst for Future Food Systems.

[44] Srinivas Kalisetty, D. A. S. Leveraging Artificial Intelligence and Machine Learning for Predictive Bid Analysis in Supply Chain Management: A Data-Driven Approach to Optimize Procurement Strategies.

[45] The Future of Banking and Lending: Assessing the Impact of Digital Banking on Consumer Financial Behavior and Economic Inclusion. (2024). MSW Management Journal, 34(2), 731-748.

[46] Paleti, S. Transforming Money Transfers and Financial Inclusion: The Impact of AI-Powered Risk Mitigation and Deep Learning-Based Fraud Prevention in Cross-Border Transactions.

[47] Polineni, T. N. S., Kumar, A. S., Maguluri, K. K., Koli, V., Valiki, D., & Ravikanth, S. (2024). A Scalable and Robust Framework for Advanced Semi Supervised Learning Supporting Universal Applications. Available at SSRN 5080654.

[48] Vamsee Pamisetty. (2023). Optimizing Public Service Delivery through AI and ML Driven Predictive Analytics: A Case Study on Taxation, Unclaimed Property, and Vendor Services. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 124-149. https://ijfin.com/index.php/ijfn/article/view/IJFIN_36_06_007

[49] Komaragiri, V. B. (2024). Data-Driven Approaches to Battery Health Monitoring in Electric Vehicles Using Machine Learning. International Journal of Scientific Research and Management (IJSRM), 12(01), 1018-1037.

[50] Maguluri, K. K., Ganti, V. K. A. T., & Subhash, T. N. (2024). Advancing Patient Privacy in the Era of Artificial Intelligence: A Deep Learning Approach to Ensuring Compliance with HIPAA and Addressing Ethical Challenges in Healthcare Data Security. International Journal of Medical Toxicology & Legal Medicine, 27(5).

[51] Annapareddy, V. N. (2022). Innovative Aidriven Strategies For Seamless Integration Of Electric Vehicle Charging With Residential Solar Systems. Migration Letters, 19(6), 1221-1236.

[52] Vankayalapati, R. K., Yasmeen, Z., Bansal, A., Dileep, V., & Abhireddy, N. (2024, December). Advanced Fault Detection in Semiconductor Manufacturing Processes Using Improved AdaBoost RT Model. In 2024 9th International Conference on Communication and

Electronics Systems (ICCES) (pp. 467-472). IEEE.

[53] Reddy, J. K. (2024). Leveraging Generative AI for Hyper Personalized Rewards and Benefits Programs: Analyzing Consumer Behavior in Financial Loyalty Systems. J. Electrical Systems, 20(11s), 3647-3657.

[54] K. Patibandla, R. Daruvuri, and P. Mannem, "Streamlining workload management in AI-driven cloud architectures: A comparative algorithmic approach," International Research Journal of Engineering and Technology, vol. 11, no. 11, pp. 113-121, 2024.

[55] Satyaveda Somepalli. (2024). Leveraging Technology and Customer Data to Conserve Resources in the Utility Industry: A Focus on Water and Gas Services. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.13884891

[56] Burugulla, J. K. R. (2022). The Role of Cloud Computing in Revolutionizing Business Banking Services: A Case Study on American Express's Digital Financial Ecosystem. Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2, 3720.

[57] Ganesan, P., & Sanodia, G. (2023). Smart Infrastructure Management: Integrating AI with DevOps for Cloud-Native Applications. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-E163. DOI: doi. org/10.47363/JAICC/2023 (2) E163 J Arti Inte & Cloud Comp, 2(1), 2-4.

[58] Venkata Krishna Azith Teja Ganti ,Kiran Kumar Maguluri ,Dr. P.R. Sudha Rani (2024). Neural Network Applications in Understanding Neurodegenerative Disease Progression. Frontiers in HealthInformatics, 13 (8) 471-485

[59] Komaragiri, V. B., Edward, A., & Surabhi, S. N. R. D. Enhancing Ethernet Log Interpretation And Visualization.

[60] Pamisetty, V. (2023). Intelligent Financial Governance: The Role of AI and Machine Learning in Enhancing Fiscal Impact Analysis and Budget Forecasting for Government Entities. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i10s(2).3480

[61] Ganti, V. K. A. T., Edward, A., Subhash, T. N., & Polineni, N. A. (2023). AI-Enhanced Chatbots for Real-Time Symptom Analysis and Triage in Telehealth Services.

[62] Daruvuri, R., Ravikumar, R., Mannem, P., & Aeniga, S. R. (2024). Augmenting Business Intelligence How AI and Data Engineering Elevate Power BI Analytics. International Journal of Innovative Research in Computer and Communication Engineering, 12(12), pp. 13012-13022.

[63] Challa, S. R. (2023). The Role of Artificial Intelligence in Wealth Advisory: Enhancing Personalized Investment Strategies Through DataDriven Decision Making. International Journal of Finance (IJFIN), 36(6), 26-46.

[64] Kalisetty, S., Pandugula, C., Sondinti, L. R. K., Mallesham, G., & Rani, P. S. (2024). AI-Driven Fraud Detection Systems: Enhancing Security in Card-Based Transactions Using Real-Time Analytics. Journal of Electrical Systems, 20, 1452-1464.

[65] Kannan, S. (2022). The Role Of AI And Machine Learning In Financial Services: A Neural Networkbased Framework For Predictive Analytics And Customercentric Innovations. Migration Letters, 19(6), 985-1000.

[66] Nuka, S. T. (2023). Generative AI for Procedural Efficiency in Interventional Radiology and Vascular Access: Automating Diagnostics and Enhancing Treatment Planning. Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi. org/10.53555/jrtdd. v6i10s (2), 3449.

[67] Ganesan, P. (2023). Revolutionizing Robotics with AI. Machine Learning, and Deep Learning: A Deep Dive into Current Trends and Challenges. J Artif Intell Mach Learn & Data Sci, 1(4), 1124-1128.

[68] Satyasree, K. P. N. V., & Kothpalli Sondinti, L. R. (2024). Mitigating Financial Fraud and Cybercrime in Financial Services with Security Protocols and Risk Management Strategies. Computer Fraud and Security, 2024(11).

[69] Challa, K. (2023). Transforming Travel Benefits through Generative AI: A Machine Learning Perspective on Enhancing Personalized Consumer Experiences. Educational Administration: Theory and Practice. Green Publication. https://doi. org/10.53555/kuey. v29i4, 9241.

[70] Somepalli, S. (2023). Power Up: Lessons Learned from World's Utility Landscape. Zenodo. https://doi.org/10.5281/ZENODO.14933958

[71] Ganesan, P. (2024). Cloud-Based Disaster Recovery: Reducing Risk and Improving Continuity. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-E162. DOI: doi. org/10.47363/JAICC/2024 (3) E162 J Arti Inte & Cloud Comp, 3(1), 2-4.

[72] Sriram, H. K., & Seenu, A. (2023). Generative AI-Driven Automation in Integrated Payment Solutions: Transforming Financial Transactions with Neural Network-Enabled Insights. International Journal of Finance (IJFIN), 36(6), 70-95.

[73] Shukla, A., Dubey, S., Nithya, P., Shankar, B., Vankayalapati, R. K., & Khatana, K. (2024). Edge-Optimized and Explainable Deep Learning Framework for Real-Time Intrusion Detection in Industrial Iot. Available at SSRN 5077557.

[74] Ganesan, P. (2024). AI-Powered Sales Forecasting: Transforming Accuracy and Efficiency in Predictive Analytics. J Artif Intell Mach Learn & Data Sci 2024, 2(1), 1213-1216.

[75] Chava, K., & Rani, D. P. S. (2023). Generative Neural Models in Healthcare Sampling: Leveraging AI-ML Synergies for Precision-Driven Solutions in Logistics and Fulfillment. Frontiers in Health Informa (6933-6952).

[76] Malempati, M. (2022). AI Neural Network Architectures For Personalized Payment Systems: Exploring Machine Learning's Role In Real-Time Consumer Insights. Migration Letters, 19(S8), 1934-1948.

[77] Annapareddy, V. N., & Sudha Rani, P. (2024). AI and ML Applications in RealTime Energy Monitoring and Optimization for Residential Solar Power Systems. Available at SSRN 5116062.