DEGREE PROJECT

Integrating Trust-Based Adaptive Security Framework with Risk Mitigation to enhance SaaS User Identity and Access Control based on User Behavior

Johnson Akpotor Scott

Information Security, Master's Level (120 credits)

2021

Department of Computer Science, Electrical and Space Engineering

Luleå University of Technology

LULEÅ UNIVERSITY OF TECHNOLOGY

Acknowledgment

Finding a topic for a thesis research work was not straightforward due to the amount of work already covered in significant areas. However, with the support of my lecturer Dr. Ali Ismail Awad, l could manage to derive a possible relevant topic as indicated in the title of this report, which is the focus of my thesis work. In addition, Dr. Ali's has been crucial to building up the thesis project. My sincere appreciation and gratitude for all his help and support.

Abstract

In recent years, the emerging trends in cloud computing technologies have given rise to different computing services through the Internet. Organizations across the globe have seized this opportunity as a critical business driver for computing resource access and utilities that will indeed support significant business operations. Embracing SaaS as a crucial business factor enhances corporate business strategy through economies of scale, easy manageability, cost-effectiveness, non-geographical dependence, high reliability, flexible resources, and fast innovation. However, this has also come with various risks due to the limitation of traditional user identity and access control solutions' inability to effectively identify and manage cloud users' authorization process when interacting with the cloud. The limit can result in a legitimate user account's impersonation to carry out malicious activities after the user account is compromised to go undetected since traditional solutions seldom function based on user behavior trust level behind any account.

Furthermore, the limitation is a significant vulnerability to the cloud environment. This vulnerability is known to be exploited by threats that can eventually lead to substantial unacceptable risks that can undermine security principles or requirements such as confidentiality, integrity, and availability. Significant consequences of this risk are categorized into financial damages, legal implications, reputational damages, and regulatory implications to the cloud environment. As a result, a solution that could contribute to the remediation of these potential risks incurred due to the limitation of user identity and access control management was proposed and designed as *User Behavior Trust-Based Adaptive Security framework*. The design aims to enhance how cloud users' identity and access control might be managed effectively based on a user behavior trust context and adaptation of corresponding access control measures through adaptive security. The design capability was manifested by integrating it into the standard ISO/2705:2018 Risk Management process. Although, there have been several good information security frameworks such as ISO/IEC 27005:2018 and other technical countermeasures such as SaaS Identity & Access Management (IDaaS) to deal with this risk on the public cloud services. However, they are based on static mitigation approaches, so there is a solid need to shift towards a more dynamic strategical approach.

The presented design work, *User Behavior Trust-Based Adaptive Security framework*, intends to serve as a proposed guideline for risk mitigation that would enhance user identity and access control limitations across the cloud. The solution functions by a trust modeling process that evaluates cloud user activities to compute a user behavior comprehensive trust degree. The resulting data is further used as input feeds parameters into a policy decision point process. The policy decision point process adapts the input parameters to user behavior trust level and behavior risk rating to determine the appropriate access control decision. Ultimately, the adaptive security solution consults the policy decision points to dynamically enforce the corresponding controls measures based on the access control decision received as input feed. The report also

conducts a risk assessment process to identify vulnerabilities, threats, and risks related to user behavior trust level and risk rating regarding SaaS resources. Then adapt the mitigation solution, *User Behavior Trust-Based Adaptive Security framework*, as a possible risk treatment within the risk management process ISO/2705:2018.

This report uses a design methodology derived from User Behavior Trust Modelling scientific research work, Gartner Adaptive Security Architecture Model, and eXtensible Access Control Markup Language's policy decision point concept. The design evaluates user behavior trust level by the trust modeling, while the integrated policy decision point processes the trust level to make the access control decision which is later enforced by the adaptive security solution. The report further adapts the risk management procedure ISO/2705:2018 to identify risk from user behavior and trust level, then implements the design solution as a possible risk treatment. The research findings were documented as Results and Discussion, where the functional and operational aspects of the designed framework were provided. In addition, the effects of applying the framework as a possible risk treatment solution were observed through conducting an ISO/2705:2018 risk management procedure. The notable outcome of a reduction of identified risk levels was an improvement in user attitude or behavior, which eventually increased user behavior trust level and reduced associated behavior risk. At the same time, the discussion detailed the interpretation of the results, implications, and limitation of the research, why the framework could be considered a remediation solution beyond the state-of-the-art for cloud user identity and access management—precisely by integrating user behavior, trust, policy decision making with adaptive security into risk management process to reduce IDM-associated risk in the SaaS.

Finally, this study has outlined the significance of adopting the designed framework as a possible mitigation solution to enhance the shortcomings of user identity and access control management in the cloud. It has demonstrated that SaaS identified risk can be reduced to an acceptable level when user behavior and activities are taken seriously. Insight into the current trust state and associated risk level of cloud users are vital for continuous risk monitoring and reduction. The solution is to be used as a recommended guideline that might significantly contribute to the research community and information security field of cloud security. Future research direction to consider the possibility of simulating and transforming this conceptual and abstract framework into a real-world working solution due to research work limitations. The framework was designed based on recognized and accepted scientific and technological principles and concepts, from user behavior trust modeling, eXtensible access control markup language, and adaptive security architecture. In addition, to extend this concept to a future research area that will focus exclusively on application-processes behavior**.**

Keywords: Risk Assessment, Security countermeasure, Risk Management, Risk Mitigation, Adaptive Security Controls, Threats, Risk, Vulnerabilities, User Behavior Trust Degree, User Behavior Risk Rating, Policy Decision Point, Policy Enforcement Point, User Behavior Trust Model, Adaptive Security Architecture, SaaS, Public Cloud.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The business goal of organizations migrating or already migrating to public cloud computing services seems to be visibly beneficial on several fronts; scalability, easy manageability, cost-effectiveness, non-geographical dependence, economies of scale, and high reliability. When focusing precisely on SaaS, major business organizations have integrated the service model as part of their business strategy, both on strategic and tactical levels. Thus, it comes as no surprise from Gartner's forecast on world public cloud revenue, according to Gartner estimates, the SaaS service model will continue to maintain dominance in the public cloud service models, with sales in 2020 expected to grow $105 billion and in 2022 will generate close to $141 billion of dollars [1]. Cloud service consumers utilize the provider's ability to host servers centrally, storage, database, network, intelligence, and software services [2]. Thus, delivering access to end-users over the Internet through a commonly used web browser, without end-users needing to install client software at affordable cost. Coupling this aspect with cloud service provider's infrastructure, applications management, and security & privacy ownership, the cloud service customer is responsible for the security of interfaces or people and data [3]. Therefore, it will undoubtedly support primary business operations for organizations subscribing to these services.

Despite these benefits, the risk to critical assets is of significant concern caused by exploits in cloud users' identity and access control management vulnerabilities. New research findings published by the Cloud Security Alliance (CSA) detailed these recent risks and challenges that can undermine the cloud's core security requirements of confidentiality, integrity, availability, authentication, authorization, accountability, and privacy [4]. In addition, commonly known vulnerabilities associated with the SaaS environment were also published in the Top 10 Web Application Security Risks [5]. Significant challenges identified through the risk assessment process become a problem for organizations adopting public cloud service when it falls out of the established risk threshold, above the risk appetite and tolerance levels established within the risk management policy. As a result, negative consequences such as financial damages, legal implications, reputational damages, and regulatory implications usually tend to be the outcome and should be remediated [6].

Current static mitigation approaches implemented through information security frameworks; System and Organization Controls (SOC) Reporting, General Data Protection Regulation (GDPR), and ISO/IEC 27017:2015 and SaaS Identity & Access Management (IDaaS), to name a few, are currently not sufficient for tackling and resolving emerging threats and risks in a dynamic environment like the cloud computing environment. Due to this limitation, researchers and several information security organizations have proposed shifting towards a more dynamic threat mitigation solution by adapting adaptive security with integrated user behavior trust context. An example can be seen in the IoT research field, where interconnected IoT nodes

conserve energy usage through adaptive security while maintaining security, another reason for shifting towards a dynamic adaptive solution. According to [7-10], adaptive security with integrated trust context will provide a real-time response, effectivity, flexibility, robustness, and self-defective to the cloud computing environment [11-15].

However, adaptive security solutions alone are not sufficient. As detailed in some research, it must function or act in a particular context, such as trust-aware, context-aware, risk-aware, etc. Thereby, integrating user behavior trust context into adaptive security solutions to adapt and enforce the appropriate access control decision accordingly might be essential to evaluate user access properly. Seamlessly supporting the enhancement of cloud user identity and access control management towards securing the fundamental security requirements of confidentiality, integrity, availability, authorization, accountability, and privacy against emerging threats [16-18].

1.1 Problem Statement

The primary security challenges identified through the risk assessment process become a fundamental problem for organizations adapting SaaS public cloud service. When risk falls out of the established risk threshold level, that's is, above the risk appetite and tolerance levels established within the risk management policy [6]. For example, the vulnerability of the user identity and access control mechanism to uniquely tie the user to their behavior before and after granting access to cloud users coupled with untrusted conduct of the user will undoubtedly lead to exploit by a threat, triggering an attack or security incidents on SaaS critical assets. In addition, compromised information security objectives or requirements can be considered a security problem. Primary sources of these problems can be associated with direct or indirect threats from the user due to malicious behavior, as expressed previously. The OWASP *Top 10 Web Application Security Risks* and *The Treacherous Twelve' Cloud Computing Top Threats in 2016* [4-5] categorized some known vulnerabilities related to SaaS, ineffective user-identity, and access management among them.

User-Identity and Access Management Issues (IAM) & SaaS Identity & Access Management (IDaaS) Vulnerability

Access layer applications such as end-user browsers with embedded java and ActiveX plugin are the main entry point to SaaS infrastructure over the Internet and can be vulnerable. Furthermore, the web application and services are not excluded from vulnerabilities due to their central role in processing and delivering SaaS services; SOAP, UDDI, WSDL, XML, REST, and HTTP [19-22]. Therefore, they are possibly prone to threat exploits and attacks.

Implementing IAM is highly significant to enforce and manage users' access in identity management, authentication, and authorization to cloud Services in a multitenant and on-demand environment. IAM technologies provide a static access control mechanism with its vulnerability

associated with major Single sign-on (SSO) technologies; OpenID Connect, OAuth 2.0, Federated identity [23-27]. Coupling with issues directly relating to users and process entities like a weak password policy, credential theft, lack of security awareness, and privilege escalation.

Limitation to handle proper cross-domain access control for multiple users and processes across multitenant diverse domains and the inability to evaluate, detect and prevent authenticated and authorized user or process entity behavior during service resource interaction for malicious activities. This is an issue due to the static nature of effectively managing user identity and access control. A compromised user identity and access control mechanism, either directly or indirectly, can lead to compromised loss of privacy, data loss, data breaches, and accountability. The emergence of IDaaS as an advanced traditional IAM solution still operates within the same static concept; entity non-behavior-based, identity, and access control management for cloud service resources usage and security. It also outlined significant security violations consequences that might result from static or inadequate user identity and access management controls regarding the security requirements of an organization's assets. Violations of confidentiality, non-repudiation, data integrity, and privacy can lead to data breaches, unauthorized data manipulation for malicious purposes like fraud, espionage, criminal intents, and copyright violations. With risk, the impact of financial losses, legal and regulations issues, and reputational damages will negatively affect an organization without adequate security controls to maintain risk to an acceptable level [6].

The outcome consequences require a Multi-layered Security Solution (Trust-based security integrated with Adaptive Security System), which is vital for a dynamic public SaaS dynamic environment. User and process behavior (trust levels) combined in adaptive security as multi-layered security mechanisms could improve users' identity and access management as part of an adequate information security strategy for decision-making. Eventually, prevent attacks and investigate threats either from legitimate authorized entities with malicious intentions or compromised authorized insider or external outsider threat agents [28].

1.2 Research Questions

Based on my literature review conducted in chapter three about adaptive security solutions with user behavior trust context, it became evident for me to research a solution that integrates user behavior trust level with an adaptive security solution coupled with policy decision making. The answer would possibly help improve or enhance the effectiveness of user identity and access control management in tackling emerging threats that can exploit cloud user entities and produce a negative risk impact on the user organization. As a result, the following research question is defined as an attempt to research this gap:

How can a trust-based adaptive security framework be integrated into risk mitigation to enhance SaaS user- identity and access control based on user behavior?

1.3 Significance of Study

The research findings will focus exclusively on designing an adaptive risk mitigation framework based on cloud user trust levels concerning their behavior before and after access was granted. In addition, the research focuses on the risks associated with untrusted user behavior and how the design framework could mitigate the risk as risk treatment through the ISO/2705:2018 risk management process.

As an input to the adaptive security system, trust attributes could aid in making the right appropriate security control decision in the SaaS public cloud. Static IAM system areas are no longer sufficient as a mitigation solution, as it relies heavily on user and process attributes of an IP address or an asset to track their activities; for example, unusual or inappropriate behavior that might be malicious by an entity (authorized or compromised) undetected immediately to take an immediate security control action.

The research outcome will be a framework as a guideline, procedure, and processes built around user trust security for adaptive security decision-making. This might support the security research community and push for more dynamic risk mitigation solutions than a traditional static solution as security controls within the SaaS cloud environment. In addition, the research will aid extending this concept further to other areas of computing and IT security practices beyond the cloud and IoT.

1.4 Scope and Limitations

A possible issue to be experienced during the process will be using a free and available adaptive security processing engine and a user behavior trust model for dynamic decision-making of the appropriate security controls within observed threat events. In addition, the Risk Monitoring and Risk Communication process will be exempted from the framework design due to the scope of the project. The possibility of finding an appropriate open-source software with integrated Artificial intelligence features to provide the adaptive security processing engine and a user behavior trust-modeling for producing a proof of concept will be challenging. Due to these reasons, the project will be a theoretical, abstract, and conceptual-based framework.

1.5 Aim and Objectives

The research project aims to design a risk mitigation framework called *Trust-Based Adaptive Security Framework based on User Behavior*. that could be used as a risk treatment solution to address emerging threats when using the SaaS resources by cloud users. The answer might

enhance the shortcoming of traditional user identity and access control management solution's inability to tie cloud users to their behavior and adapt the corresponding access control to reduce identified risk to an acceptable level. The answer is tested or used within the Risk Management ISO/2705:2018 process as a risk treatment mitigation solution. This would resolve the reach question: “How can a trust-based adaptive security framework be integrated into risk mitigation to enhance SaaS user- identity and access control based on user behavior?”

To achieve this aim, the following two sets of objectives will be performed as part of the Risk Management ISO/2705:2018 process, as in figure 1.

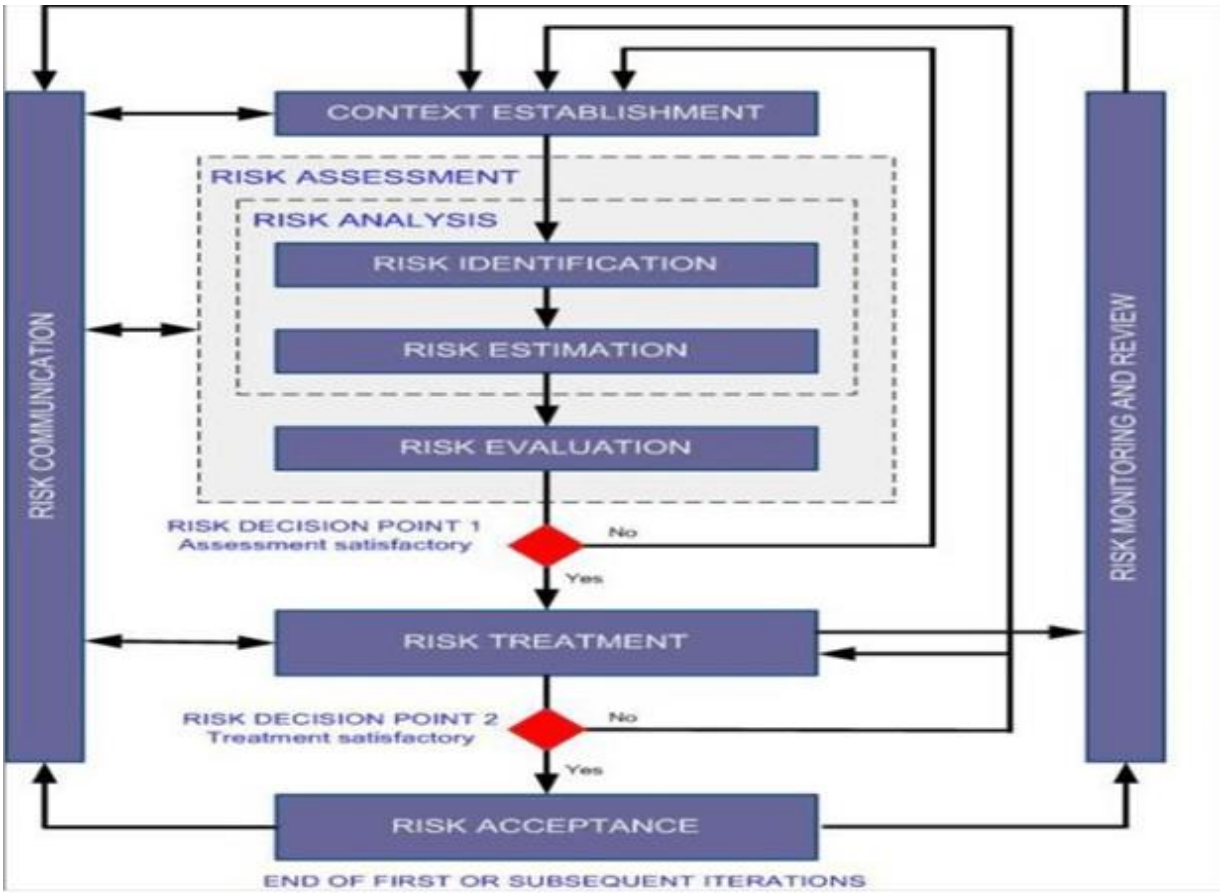


Figure 1 ISO/IEC 27005:2018 Risk Management process [29].

Develop or Design: *Trust-Based Adaptive Security Framework based on User Behavior*. The User behavior trust evaluation by trust model, policy decision-making, and an adaptive security solution for security control enforcement function as policy enforcement points.

Implementation *Trust-Based Adaptive Security Framework based on User Behavior***.** As mitigation solution in Risk Management process ISO/2705:2018*:*

- Context establishment and Risk Tolerance and Threshold Statement for SaaS
- Risk Identification centered on cloud user entity.
- Risk Estimation; Qualitative approach
- Risk Evaluation based on Risk Appetite, Tolerance, and Threshold
- Risk Treatment implementing " Trust-Based Adaptive Security Framework based on User Behavior’’ solution.″
- Risk Acceptance Evaluation: Risk acceptance criteria derived from Risk Appetite statement and Risk Tolerance Statement.
- Risk Monitoring and Risk Communication; omitted as stated in Scope and Limitations

Chapter 2

Background: Cloud Computing, Adaptive Security Architecture, and Trust-Based Security

2.1 Cloud Computing Overview

This section describes a general overview of the cloud computing concept without diving deep into how the underlining technologies work. Additional section *SaaS Public Cloud Computing* outlines the SaaS cloud service model specifics.

2.1.1 Definition of Cloud Computing and Characteristics

The official definition of Cloud Computing, according to NIST, is "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [30].

IS0/IEC also proposed other definitions as a "Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand" [31].

The benefits and essentials of cloud computing were further detailed by [32] outlined in figure 2, "Essential characteristics of cloud computing" [33], consisting of; On-demand self-service, Broad network access, Multi-tenancy, resource pooling, Rapid elasticity, and Scalability measured Service.

On-demand allows the provisioning and de-provisioning of cloud resources by cloud service customers without human intervention from the cloud service provider. For example, resource provisioning; database instances, virtual host or server's instances, storage space, and web self-service portal interface to cloud services accounts and usage without provider intervention.

Broad network access supports cloud computing resources access across the Internet for public cloud and local network for private cloud. However, this also concerns the quality of services - both on the link and services delivered across this broadband connection and local area network.

Multi-tenancy and resources pooling is the ability for multiple cloud customers to share the same or single cloud physical resources or applications. Sametime maintains data security and privacy that allows numerous operations or simultaneous operational environment coupling with resources pooling from multiple customers on the same resources.

Resources reservation for resources pooling must be planned and managed adequately by providers to avoid denial of services and performance degradation issues. Rapid elasticity and scalability should be regarded as the landmark signature characteristics of cloud computing. It provides the ability for cloud resources to be rapidly provision and de-provision when and after the resources have been used, such as virtual machines, storage, and customer applications.

Coupling with scalability, the customers can have the possibility to plan for future resources allocation or expansion gradually, scaling up or scaling down within affordable cost and when needed. Thus, scalability supports the opportunity of economic scale management for the customers. Measured service monitors and measures the resource usage of cloud service resources consumers, similar to any other services, where customers have to pay for service consumption. Thus, enable the means for cloud service providers to gain income or financial benefits for their service provision.

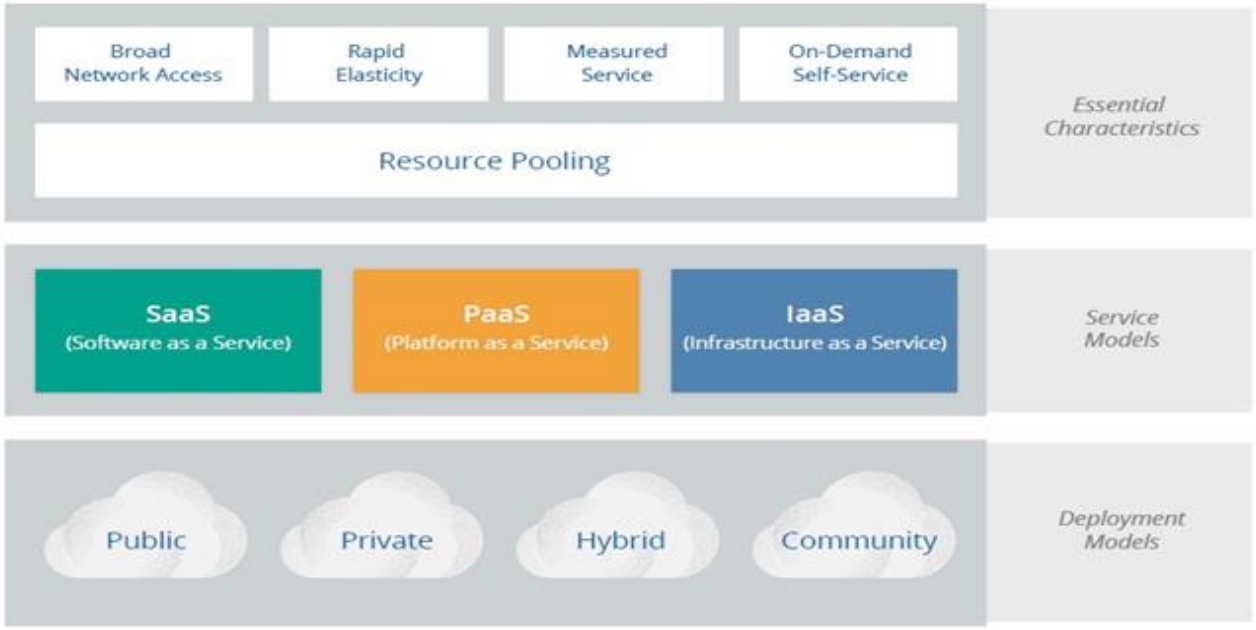


Figure 2: Essential characteristics of cloud computing [33].

NIST further provides a standard architectural and taxonomy reference model of cloud computing, which defines different roles, activities associated with each position, and central subcomponents of each layer of the reference model as in figure 3, *the conceptual reference model* [34].

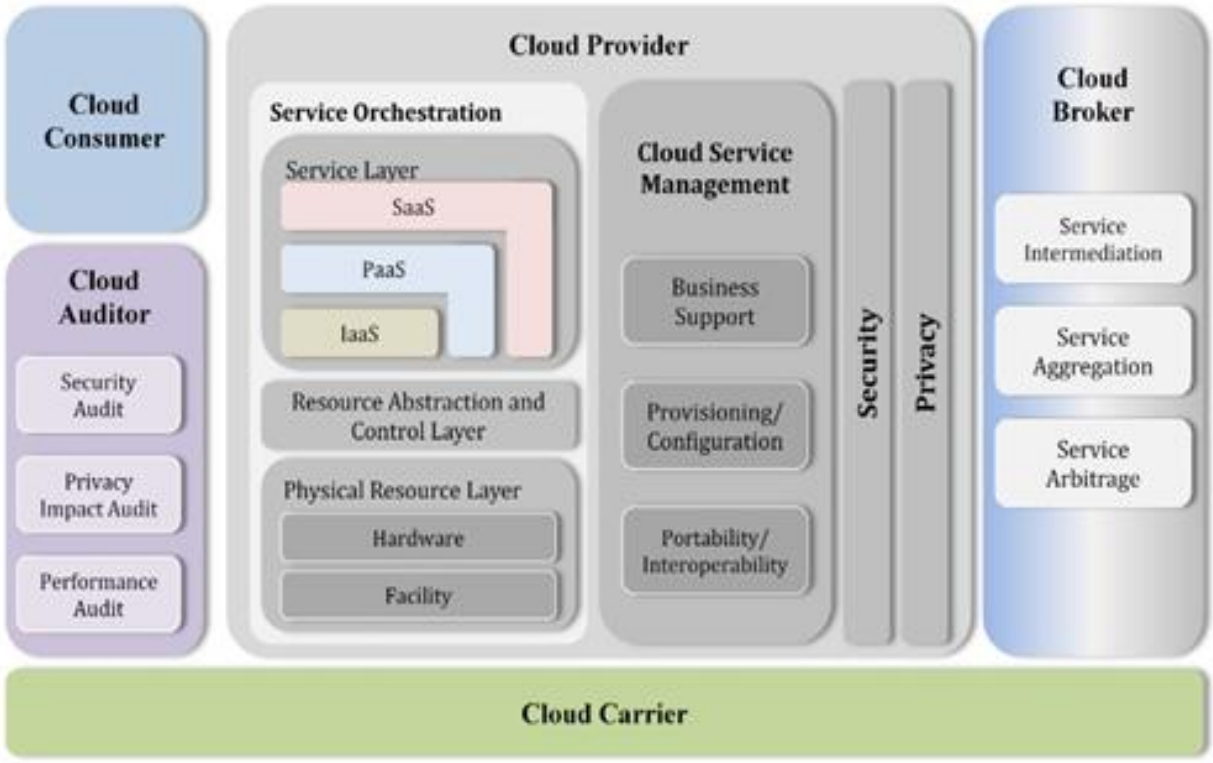


Figure 3: NIST cloud reference conceptual architecture model [34].

The model defines the function of each role and each corresponding layer component:

- Cloud Consumer – A business entity that maintains a business relationship with cloud providers and subscribes to provider service.
- Cloud Provider- A business entity that provides cloud service to cloud consumers.
- Cloud Auditor- A party that independently conducts risk assessment of cloud service, information system operations, performance, and security of implemented cloud service.
- Cloud Broker - An entity that liaises between the cloud provider and cloud consumer in business relationships and manages the quality assurance or quality of Service of the cloud services delivery.
- Cloud Carrier - is intermediary connectivity and transport of cloud services from cloud provider to cloud consumers.

[34] detailed the cloud services available to the cloud consumer as in figure 4, *Services Available to a Cloud Consumer.*

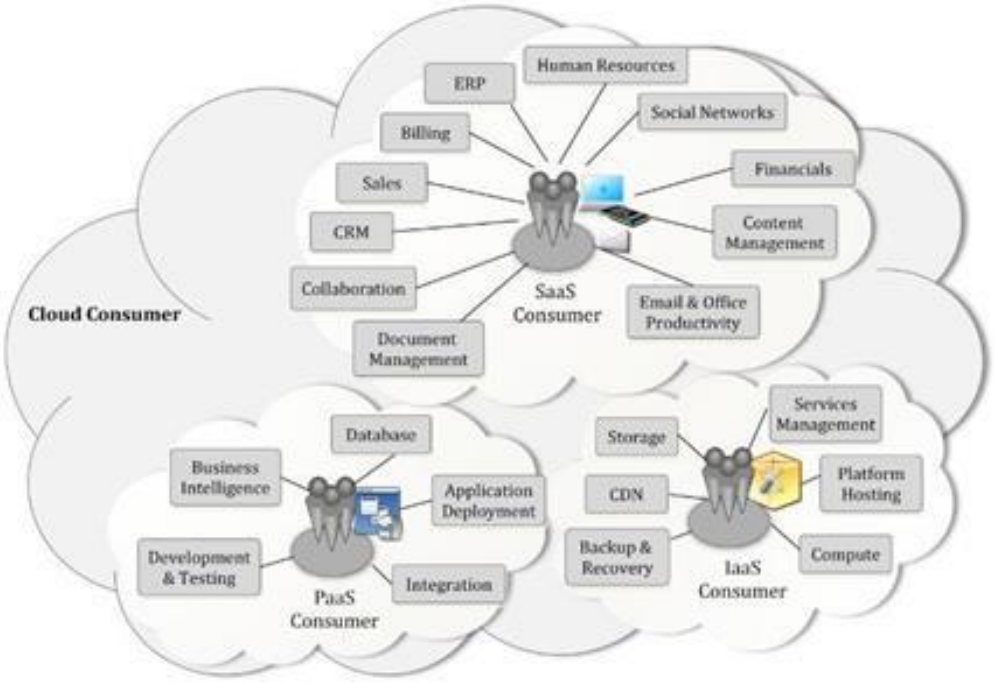


Figure 4: Services Available to a Cloud Consumer [35]

2.1.2 Cloud Service Shared Responsibility Model

The shared responsivity model detects both cloud service consumers and providers; it can be a grey area concerning who does what. For example, according to [34], splitting control of the security responsibility of the cloud services means both parties must share the responsibility of protecting the cloud. While [35] explicitly provides in-depth details of the separation of functions between the two entities.

The cloud services consumer is responsible for "Information and data protection, Application Logic and code protection. Identity and Access control with; user identity and access management (IAM), single sign-on (SSO), multi-factor authentication (MFA), access keys certificate, user creation processes, and password management" [35]. In contrast, the cloud service provider will be responsible for the Virtualization Layer security of resource provisioning management. Provisioning storage, CPU, GPU, and memory allocation through virtualization. In addition to physical hosts, network, and datacentre logical and physical protections to ensure high availability through redundancy, backup, and restore process for business continuity and disaster recovery management. [35].

The grey area security happens either when IaaS or PaaS service model is used, depending on the agreed services contract terms. Functions that fall within the grey areas, according to [35], consist of; Identity and Directory Infrastructure, Applications, Network Controls, and Operating systems.

2.1.3 Cloud Computing Enabling Technologies

Enabling technologies are the core underlining technologies that support the cloud services' functionality; Broadband networks and internet architecture, fundamental data transport medium, where ISP providers convey data across several internet backbones interconnected with cores routers operating in connectionless packet switching and router-based interconnectivity for end-to-end packet forwarding. Data Centre Technology is the computer system and related component hosting facilities, including network systems, telecommunication, and storage equipment. Its key features consist of both physical and virtualized IT resources, as presented in figure 5.

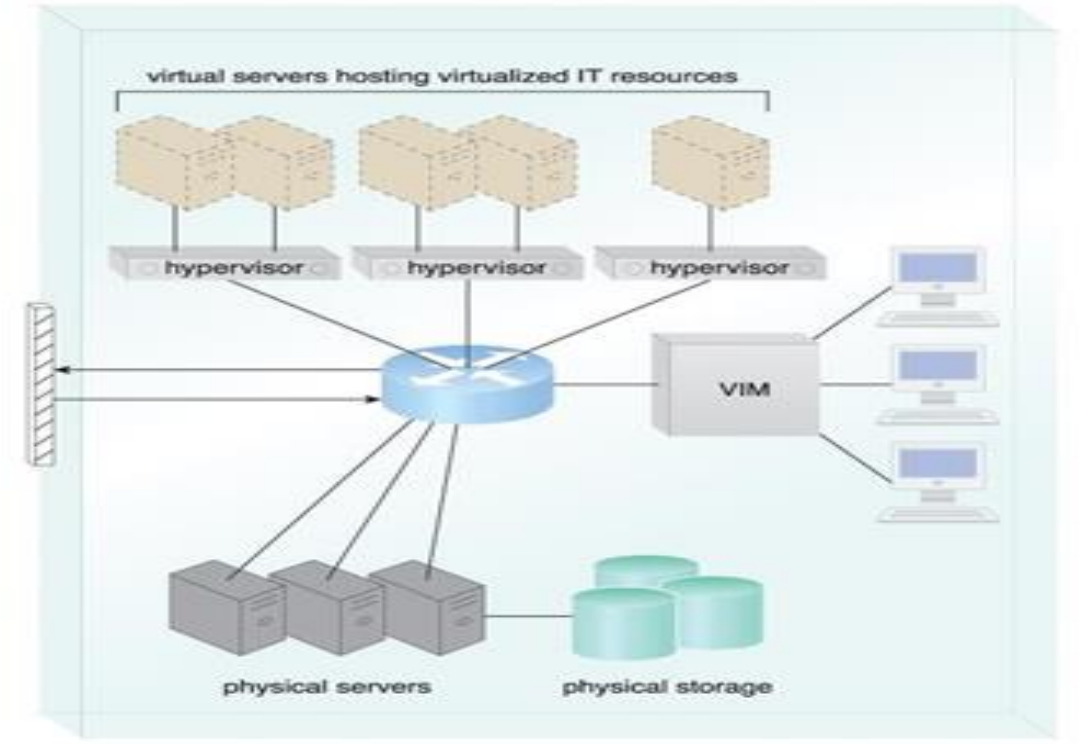


Figure 5: Virtualized IT resources supported by physical IT resources. [36].

Central enabling technologies are standardized hardware and modular technologies, aggregating identical blocks of infrastructure and equipment that support scalability, growth, and speedy hardware replacement—automation for resource provisioning, configuration, system monitoring, and patch management. Remote operation and control for IT resource operational and administrative tasks. Virtualization technology converts physical resources into virtual IT resources such as storage, network, server, and power [36-37]. Due to its ubiquity, Web technology is commonly used as the front-end application for cloud consumers, cloud service

implementation, and remote management of the cloud IT resources. A common implemented web application is based on service-oriented architecture and web services; SOAP, HTTP, REST, XML, WSDL, UDDI, HTML, and URL [36-38] as in figure 6 Basic architectural tiers of Web applications.

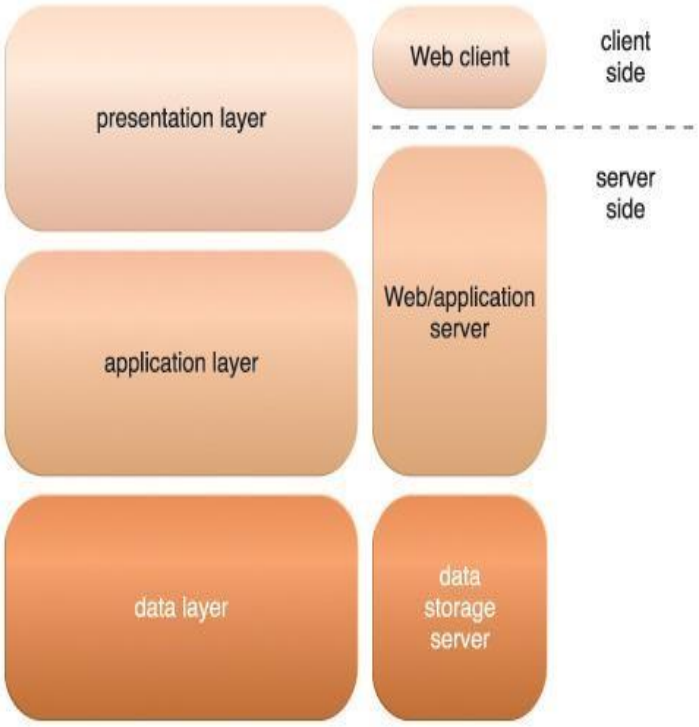


Figure 6: Basic architectural tiers of Web applications. [39].

Multitenant Technology presented in figure 7 enables cloud consumers to access and use a commonly shared application or resources and individual data and configuration simultaneously without undermining security privacy. Each tenant can individually customize shared applications such as User interface, Business Process, Data Model, and Access control with typical characteristics of multitenant applications: data security, usage Isolation, Recovery, application upgrades, scalability, metered usage, and data tier isolation. [36].

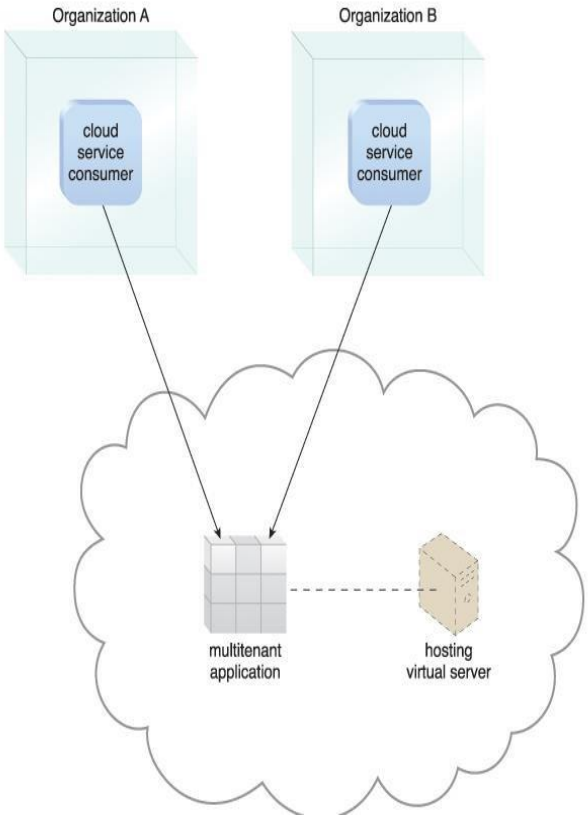


Figure 7: Multitenant Technology [36].

Containerization is the process of deploying individual isolated applications and cloud services within a single operating system. The process involves virtualizing the operating system resources on a single physical server or virtual Service for each application and cloud service while maintaining privacy [36].

2.2 Cloud Service Models

According to NIST special publication 800-145, cloud defines and categorizes cloud computing service model as the following:

2.2.1 Software as a Service (SaaS)

"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure" [30]. The client has no responsibility for managing the underlining infrastructure

or risk and has no control or ability to influence it. Section 2.5, *SaaS Public Cloud Computing*, provides in-depth technical details, while figure 8 shows SaaS services and applications examples. [40]

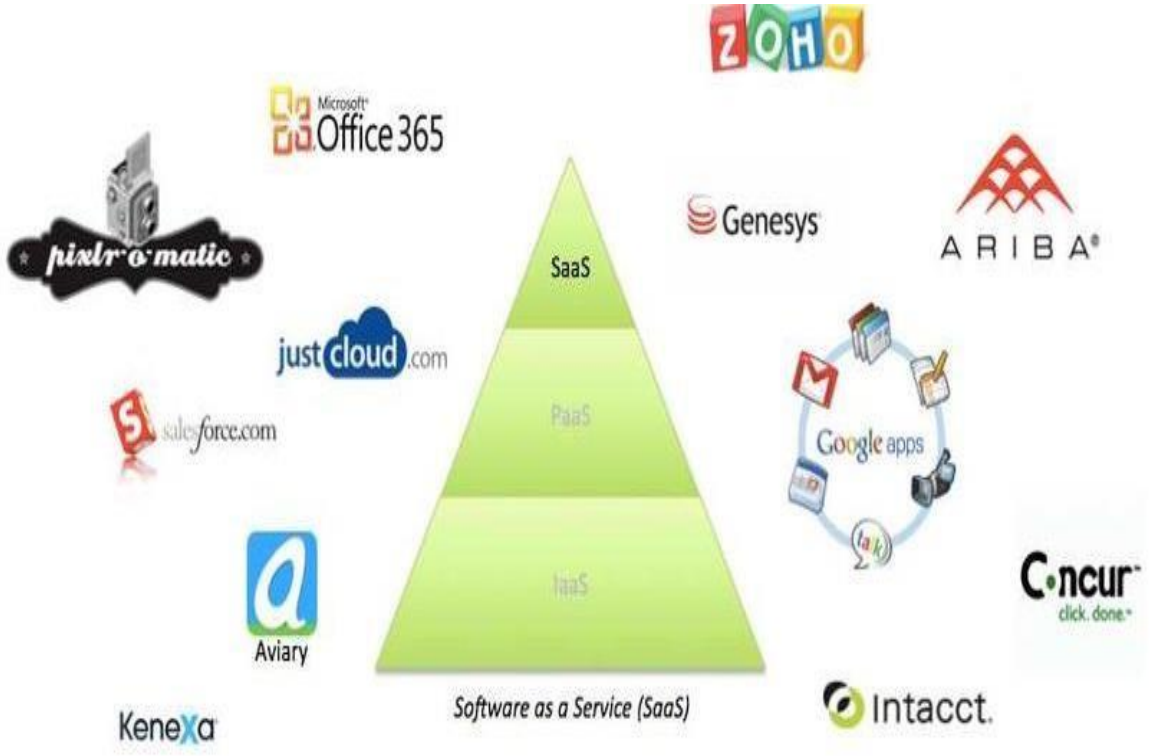


Figure 8: Examples of SaaS service and application [40]

2.2.2 Platform as a Service (PaaS)

"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider." [30]. Managing the underlining infrastructure in risk and system administration can be a shared responsibility between the customer and the provider. Figure 9 shows examples of PaaS services [40].

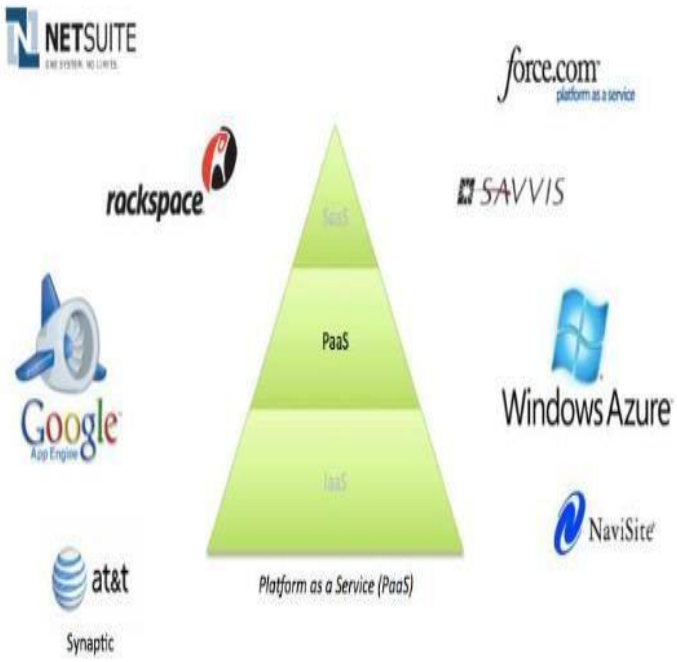


Figure 9 shows examples of PaaS services [40]

2.2.3 Infrastructure as a Service (IaaS)

"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications." [30]. Like PaaS, infrastructure and Risk management can be a shared responsibility between customer and provider. Figure 10 shows examples of IaaS services [40].

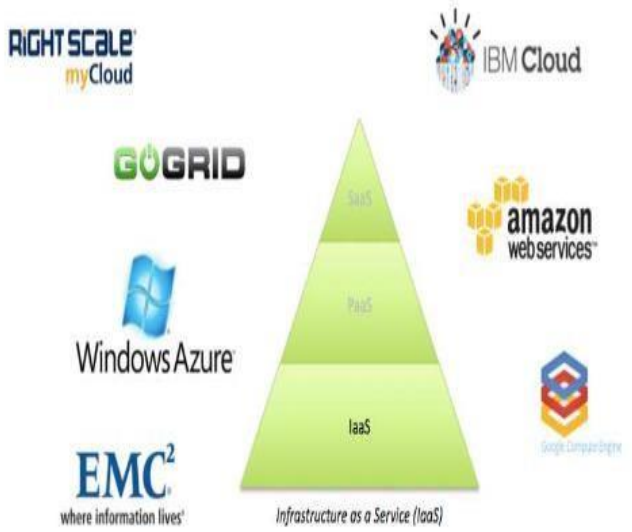


Figure 10 shows examples of IaaS services [40].

2.3 Cloud Deployment Types

NIST Special Publication 800-145 also classify the following deployments type with each specific feature represented as a graphical representation of the deployment as in figure 11[30].

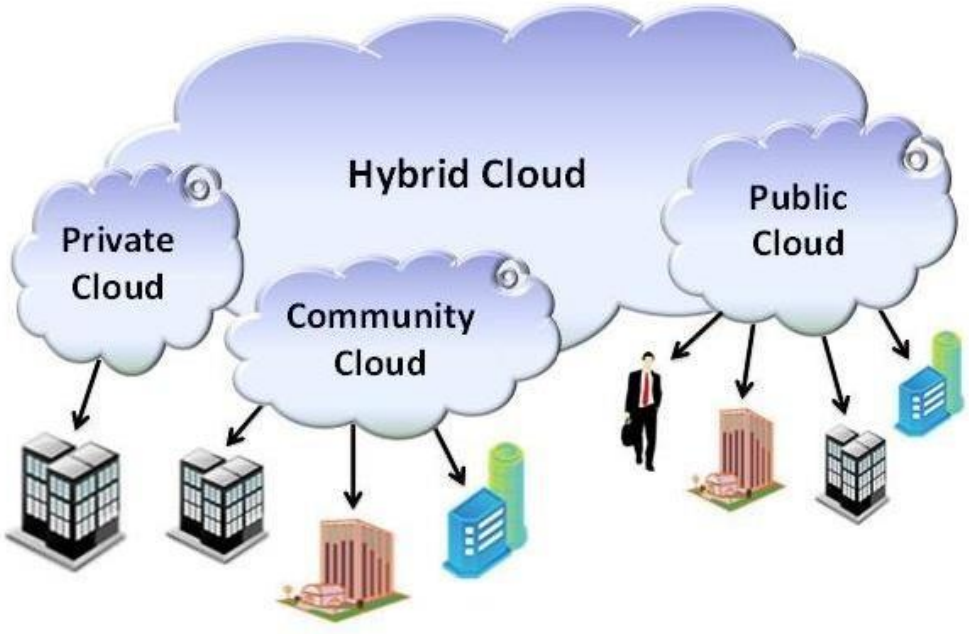


Figure 11: Cloud Computing Deployment Models [30].

2.3.1 Private cloud.

"The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units)" [30]. It can be hosted and managed internally by an organization or a cloud service provider. Private cloud falls short of the economic benefits in terms of the cost that cloud computing provides, but security can be seen as the main benefit of this model.

2.3.2 Community cloud.

"The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)." [30]. Hosted and managed internally by an organization or by a service provider. Cost-effective by spreading the cost among the trusted community. Provides some level of security assurance and is cost-effective.

2.3.3 Public cloud.

"The cloud infrastructure is provisioned for open use by the general public." [30]. Hosted and managed solely by the service provider, cost-effective but with security limitations for a secured cloud environment.

2.3.4 Hybrid cloud.

"The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability" [30]—considered as the best solution among the solutions. Ensure cost-effectiveness and a high level of security assurance, mostly when combined with private and community cloud solutions.

2.4 Security Requirements

Major security requirements consist of confidentiality, integrity, availability, authentication, authorization, accountability, and privacy for cloud computing. In addition, the requirements should be protected against compromises from threats.

2.4.1 Risk Associated with Cloud Computing

As stated by [6], these benefits of cloud computing services are also associated with financial damages, legal implications, reputational damages, and regulatory implications due to incurred risk because of emerging threats exploiting user-entity and system vulnerabilities.

2.4.2 Cloud Services and Business Continuity

As indicated in one IBM cloud service journal, "Over the last couple of years, we have seen the emergence of cloud providers that provide disaster recovery as a service (or DRaaS, if you like). They provide a complete service that can handle your disaster recovery, provided you stay within their stated constraints" [41]. However, disaster recovery is not the only control framework for security readiness. And should be combined with other controls such as risk management.

2.5 SaaS Public Cloud Service

SaaS is a software delivery model where centralized hosted software and applications are distributed and made available to the cloud service customer over the Internet. Typical providers of SaaS cloud service consist of Microsoft Azure by Microsoft, Amazon AWS by Amazon, Salesforce, Zoom, Slack, Nextiva, Google Cloud, Shopify, Atlassian, Mailchimp [42-43] shown in figures 12 and 13, with each provider's related services. Most SaaS services and applications made available to cloud services customers do into two varieties according to [42-44].

- Vertical SaaS that provides software for industrial needs or business needs, for example, healthcare, agriculture, finance industries,
- the Horizontal SaaS provides software that focuses on software categories for industries functions such as marketing, Sales, Human Resources, collaboration, customer relationship management (CRM), management information systems (MIS), enterprise resource planning (ERP), human resource management (HRM).

Figure 12: Major SaaS providers [42-43]

Provider	Services
Salseforce.com	On-demand CRM solutions
Microsoft Office 365	Online office suite
Google Apps	Gmail, Google Calendar, Docs, and sites
NetSuite	ERP, accounting, order management, CRM, Professionals Services Automation (PSA), and e-commerce applications.
GoToMeeting	Online meeting and video-conferencing software
Constant Contact	E-mail marketing, online survey, and event marketing
Oracle CRM	CRM applications
Workday, Inc	Human capital management, payroll, and financial management.

Figure 13: Major SaaS service provider and services [42-43]

According to Cloud Security Alliance, cloud computing such as SaaS offers many benefits in terms of agility, resiliency, and economy, no hardware provision, limited downtime due to the elasticity nature of the underlining infrastructure. Limited or little capital expenditure in system maintenance and security implementation due to provider service operation ownership [33-37].

With SaaS, the underlining infrastructure such as the data center facility, network, firewalls, server storage, operating systems, and developer's tools are owned and managed by the cloud services provider. As a result, all the cloud services the customer is concerned with are centralized hosted applications, entity account management, data security, and privacy management.

Hosted application subscription and usage are generally based on the pay-as-you-use billing concept. That can be accessed through the web application and interface layer or thin-client, usually web browser to hosted applications. However, not all applications are customizable, like office 365 or the entire Microsoft office package. In this case, customers can develop their customized applications through the SaaS application programmable interface.

Other benefits of subscribing to SaaS include efficient software licensing usages where single licenses are shared by multiple users, centralized systems and data management, and multitenant solutions. In addition, the section *Cloud Computing Enabling Technologies* outlined the underlining technology that provides the operational backbone of the SaaS cloud services.

2.5.1 SaaS Entity Management and Access Control (Identity and Access Management (IAM), Identity-as-a-Service (IDaaS), and Cloud Identity Management).

Gartner defines IAM as "The security discipline that enables the right individuals to access the right resources at the right times for the right reasons." [45]. SaaS entity access control and management to cloud resources has shown advances from the traditional approach of premises-based Identity and Access Management (IAM) and moved on from just extending Active Directory to developing a complete cloud solution known as the new generation of IAM Cloud Identity Management. They shifted the authentication, authorization, administration of Identities, and audit to the cloud. Initially kicked off Identity-as-a-Service (or SaaS IAM) but still effectively single-sign-on to web applications solution before complete cloud-based IAM solution [46].

The core functional goal of both solutions mostly remains the same but with slight variants of underlining technologies and standards, in conjunction with a significant exception of cloud identity management, making it a full-blown cloud-based IAM solution.

According to [46], Cloud identity management is a modern adoption of Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) with the associated add-on of web application SSO, MFA, PAM, and IGA. Significant benefits argued by [46] stated that this new generation SaaS IAM or IDaaS enable cloud service providers to provide the following identity and management features such as; employees secure connection to their devices, IT applications on premised and cloud, cloud and premised hosted files, and network through VPN and WiFi connections, leveraging of zero-trust principles, entity management overhead

limitations. In addition to securely connecting cloud servers such as AWA, Google Cloud, Microsoft Azure to cloud customer LDAP and AD user store, manages various operating systems, laptop, desktop, and mobile devices regardless of location, LDAP and AD extension to the cloud, supports for system and applications multi-factors authentication, SAML-based authentication.

According to the Cloud security alliance, the critical underlining identity and access management standards technologies remain the same. Still, with newly defined standards, such as: "Security Assertion Markup Language (SAML) 2.0 is an OASIS standard for federated identity management that supports both authentication and authorization. OAuth is an IETF standard for authorization widely used for web services (including consumer services). OpenID is a standard for federated authentication that is widely supported for web services. It is based on HTTP with URLs to identify the identity provider and the user/identity (e.g., identity.identityprovider.com). Extensible Access Control Markup Language (XACML) is a standard for defining attribute-based access controls/authorizations System for Cross-domain Identity Management (SCIM) is a standard for exchanging identity information between domains, federated identity management system and SSO." [47-48]. Identity and access management services of cloud users and processes entity are still built around the core access control principles according to [48] SECaaS implementation guidance of IAM should consist of components; identity management, entitlement, authentication, authorization; Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), Discretionary access control (DAC), Mandatory access control (MAC), rule-based Access Control, separation of duties, need to know, and least privilege principles.

2.5.2 SaaS Security Issue

The key to understanding SaaS security issues is first understanding the common vulnerabilities associated with SaaS services and applications. This then forms the basis for identifying the threats and outcome risk because the threat exploits these vulnerabilities. For example, the OWASP® Foundation [5] listed the following Top 10 Web Application Security Risk as vulnerabilities:

- Injection -The injection of malicious code or data web application to behave unexpectedly.
- Broken authentication -Wrong authentication configuration and management process can lead to credential, session token breaches commonly used for identity theft.
- Sensitive data exposure -Sensitive data exposure vulnerability can prevent data breaching with personal information theft like personally identifiable information, credit card details, and security numbers commonly used for impersonation and fraudulent activities.

- XML external entities (XXE) -Poorly configured or outdated XML L processors can allow remote code execution, denial of service attack, port scanning, unauthorized files read and write due to processors' Evaluation of external entity references within XML documents.
- Broken access control - Improper enforcement of access control can allow attackers to access sensitive information, for example, password, sensitive files, libraries, applications that are supposed to require secure access.
- Security misconfiguration -Issues that can arise from operating systems and services with misconfiguration or system default setting such as default account, default system settings, protocols, and files can lead to several security issues.
- Cross-site scripting (XSS) -XSS flaw resulted from poor coding of the CGI script, familiar gateway interface of the web application when input data was not correctly validated and sanitized by the web application when receiving this data. Such a flaw can lead to malicious script execution, session hijacking, website defacement, and redirecting a malicious website. Attacks can take place within the user browser or the web server itself.
- Insecure deserialization -Like XSS, poor or improper input validation and sanitization can lead to remote code execution, injection attacks, replay-attacks, and privilege accounts escalation.
- Using components with known vulnerabilities. -Unpatched outdated software components such as code libraries, processes, software modules, a framework that runs with privilege account. Being exploited can lead to different security attacks, such as remote code execution, system takeover, data loss, system data breaches, and denial of services.
- Insufficient logging and monitoring -Inadequate or lack of insight into network, system, processes, and users' activities because of unimplemented logging and monitoring systems or mechanisms will allow malicious activities or events to go unnoticed, leading to several security incidents.[5].

The above vulnerabilities in SaaS services are not enough to compromise the Service. There must be related threats for this to occur. According to *The Treacherous Twelve' Cloud Computing Top Threats in 2016* [4], more recent threats were identified and published in addition to [49] *Cloud Security Challenges in 2020* publication of similar threats commonly found in SaaS service. List of Threats posted by *The Treacherous Twelve' Cloud Computing Top Threats* in 2016 [4] consists of the following:

- Data Breaches -Data breaches resulting from loss of confidentiality can lead to the exposure of sensitive, confidential, or protected data into the hands of an unauthorized person or process, which can then be used for malicious purposes.
- Weak Identity, Credential, and Access Management -The access of legitimate cloud users' accounts to malicious actors facilitates the means of compromising cloud resources

without proper access credential management for origination cloud deployment, the ease of this type of attack.

- Insecure APIs -Coding errors and improper data validation and sanitization of API (whose main task is to interact with backend application services when exploited) can lead to loss of security protection of both backend and client process interacting to deliver services, such as automating cloud services, cloud service delivery.
- System and Application Vulnerabilities - When vulnerability due to coding errors or bugs in software and applications are not patched, it tends to be an accessible channel for system compromise. The question comes if this vulnerability is exploited or not. A cloud instance with vulnerability can lead to a lateral actor on another instance if the underlining system's proper security measures are compromised.
- Account Hijacking - Compromised cloud users' accounts are frequently common if not correctly protected either through security awareness training or through multi-factor authentication mechanism against session hijacking, phishing of funds, and attacker using this to access sensitive data or conduct literal attacks or further attacks on the cloud resources.
- Malicious Insiders - Most times, organizations focus on external threats without considering insider threats. However, insider threats can significantly threaten the organization's resources due to privileged access rights. For example, a malicious insider with system administrative privileges such as disgruntled employees; can act maliciously against organization cloud resources when having the opportunity.
- Advanced Persistent Threats (APTs) - Well-organized malicious actors with the support of a financially equipped organization or government can conduct highly motivated attacks such as sabotage, massive data exfiltration, or patent theft for considerable financial gain or destruction. This type of attack tends to be stealthy, sophisticated, persistent in nature, which can go undetected for an extended period.
- Data Loss - Data loss due to data breaches, malicious agents, or accidental action like wrongful write privilege assignment or accidental deleting of critical files can negatively impact an organization's business operation, for example, the loss of sensitive information regarding the business operation or dealings.
- Insufficient Due Diligence - The responsibility for senior managers to show governance and take the appropriate decision for migrating to the cloud is a significant step, which will avoid making a service contract with the wrong or incompetent cloud service provider. An example can be verifying if cloud service provider adheres to relevant security framework or standards, conducting risk assessment, etc., to secure their cloud environment. Lack of such a control process can be detrimental when using the cloud for business operations.
- Abuse and Nefarious Use of Cloud Services - The benefits of cloud computing have not only benefited legitimate organizations when conducting business operations, but it has also benefited malicious actors to conduct malicious activities, for example, using the

cloud to launch denial of service attacks, hosting malicious domains and websites for malware distribution, Command, and Control Centre, lurching phishing attack and spam distribution.

- Denial of Service - Cloud computing and customers can become victims of this attack. Cloud provider infrastructure can be used in launching DDOS attacks, and likewise, compromised cloud customers systems can be used as the source of an attack. Both entities as potential targets.
- Shared Technology Issues - Shared resources or infrastructure of cloud computing is one of the significant characteristics of cloud service. Being a multitenant environment for multiple organizations service subscription and usage on same resources, the lack of security control and insecure isolation of each resource in underlining virtualization deployment can lead to information leakage, lateral attack, or pivoting from one organization resource domain to another. It can eventually lead to security breaches or compromise.

2.5.3 SaaS Security Challenges in 2020

According to [49], the publication of these recent challenges is a mixture of existing threats published in [5] but with the incorporation of some newly identified threats recently observed in the cloud environment. The following list details only the threats not covered in [5]; data Breaches, Insufficient Identity, Credentials, Access, and critical management account hacking.

2.6 Adaptive Security Architecture

[14-15] Proposed the definition and functionality of Adaptive security as a "Security model in which the monitoring of threats remains continuous and improves as cybersecurity risks change and evolve." The system's functionality heavily relies on advanced machine learning and artificial intelligence (AI) elements that extend this analytical approach to security. As shown in figure 14, the Adaptive security architecture comprises four functional stages for event monitoring and process based on defined criteria—finally, the appropriate adaptation and decision taken against identified or unknown threats.

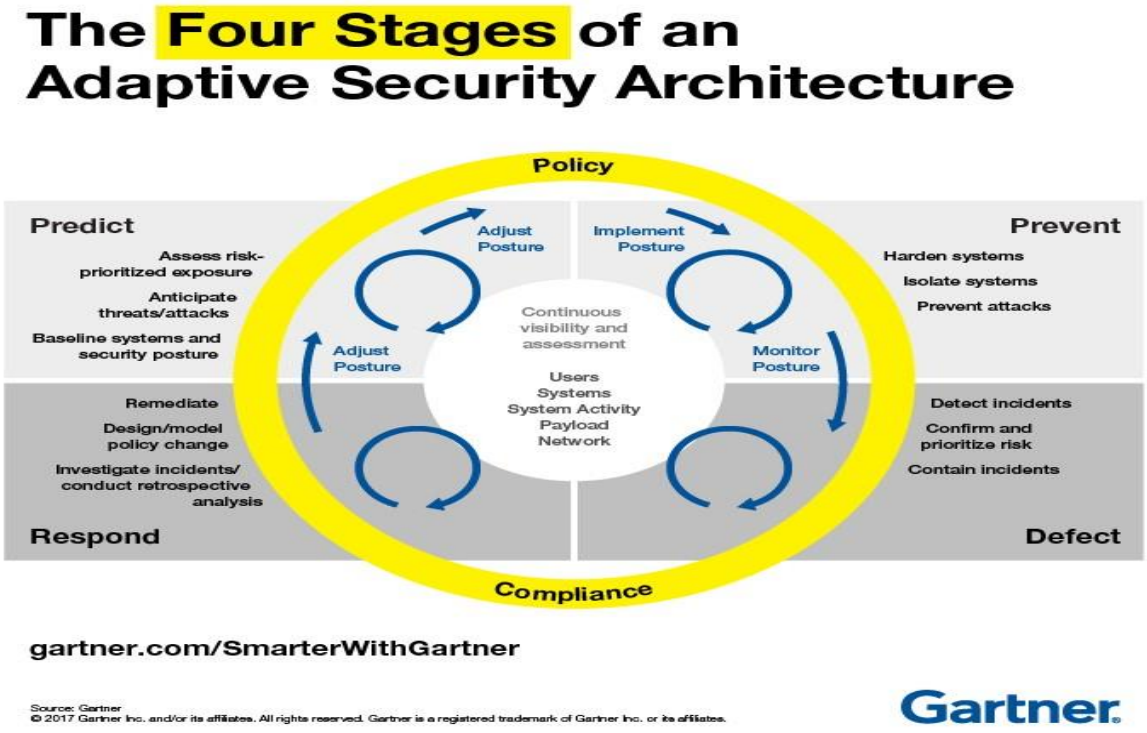


Figure 14. The Four Stages of an Adaptive Security Architecture [14-15]

[14-15] Also briefly describes the four functional stages of Adaptive Security Architecture as follows:

- Predict - Prediction of anticipated threat and risk, malware and possible attacks, and security baseline and posture implementation.
- Prevent – Identified and unknown threats and attacks, system hardening, security policy enforcement, and threat intelligence utilization as preventive support against security requirement compromise.
- Respond – Implement incident response procedure, policy design changes and perform investigate incidents, policy changes adaptation, and design, utilization of threat intelligence as response support.
- Detect – detect incidents, confirm, prioritize risks, and contain incidents.

2.7 Trust-Based Security

2.7.1 Overview of Trust Concept

The concept of trust highlighted in the past decade was applied in distributed artificial intelligence. Still, more research areas are adapting this approach to enhance adequate security controls as a risk-mitigating mechanism against an emerging threat by focusing on the reputational aspect of entity behavior when using computing resources.

As stated in one of [50] research works, trust-based base reputation; in other words, behavior, when used as a trust-enforcing mechanism during the e-commerce transaction, will act as a control measure to avoid frauds or cheaters. More of these approaches are currently observed in the IoT research area, where trust reputation or behavior concept is now integrated into Adaptive solutions to produce dynamic adaptive decision-making for IoT node energy conservation.

However, how do trust definition applied to the information technology context? An excellent insight was proposed by [51], defining trust-based by encompassing several trust studies across different domains, such as sociology, psychology , politics, and business science . His definition was "Trust is a subjective assessment of another's influence in terms of the extent of one's perception about the quality and significance of another's impact over one's outcomes in a given situation, such that one's expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation." [51].

Trust and Reputation as a social value were emphasized by [52] as an essential fact for building a high level of probability of good collaboration or not due to trustworthiness. Social and psychological factors included further thoughts on the trust concept *Formalizing Trust as a Computational Concept* [53] on the trust model.

2.7.2 Trust-Based Security Attribute – (User Behavior)

Adapting user behavior trust context might help overcome the drawback of user identity and access control management for mechanisms such as Identity and Access Management (IAM), Identity-as-a-Service (IDaaS), and Cloud Identity Management when accessing and utilizing SaaS resources access. Trust-based adaptive security that relies on the user's behavior and assigned trust level could be the right direction to take. [54] Also signified in the context of intelligent and adaptive environments, efficient trust evaluation or behaviors analytics of user entity will serve as a security parameter for adaptive decision-making [16-18]. The adaptive decision-making forms the basis for appropriate mitigation control against threats and risk [13-15] across the SaaS environment. [16] The essential trust-based security "trust attributes" are presently suitable for adaptive solution integration to aid decision-making, as in figure 15.

Taxonomy of trust consists of service-based trust, Context-based trust, Attribute-based trust, and policy-based and Entity based trust. Trust attribute is relevant to my research project and will rely on Context-based trust "Behaviour/User Context." In some information security articles, the naming of trust attributes can be slightly different: for example, applied by [55] User and entity behavior analytics (UEBA), also known as user behavior analytics (UBA)," but the primary or fundamental principle remains the same. It evaluates user entity behavior concerning computing resources to determine whether it is malicious, poses a threat, and prompts immediate investigation.

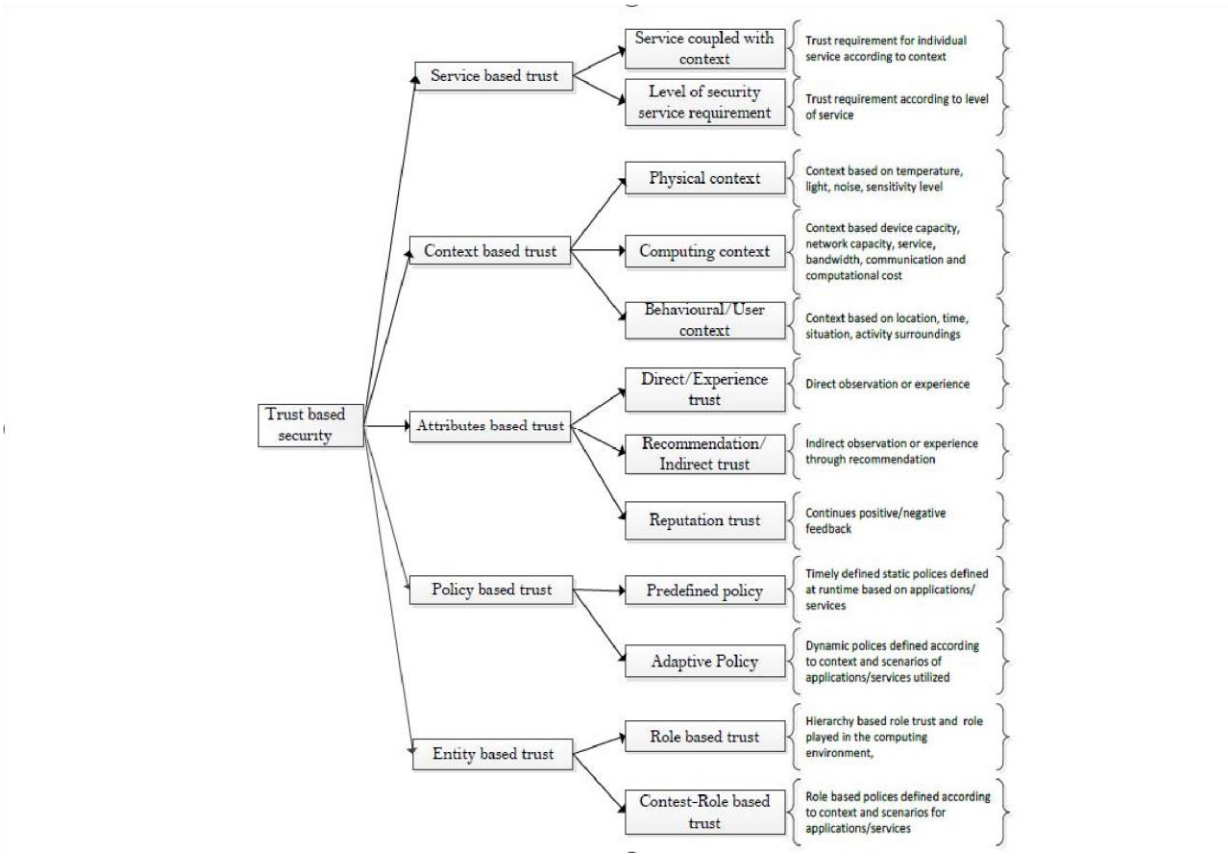


Figure 15: Trust-based security parameter [16]

For this thesis project, trust-based security parameters will preferably be [16] extracts from the trust-based classification and attributes as represented in figure 16.

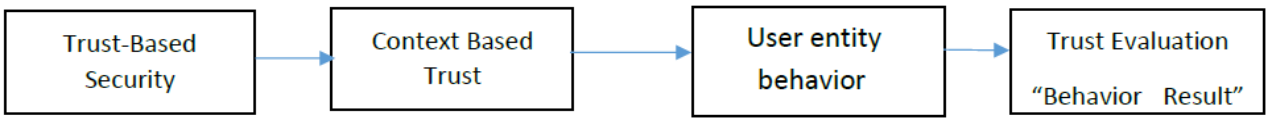


Figure 16: Trust-based classification and attributes

According to [55], user and entity (UEBA) behavior analytics, otherwise known as user behavior analytics (UBA), "Is the process of gathering insight into the network events that users generate every day. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behaviors". However, user and process entities constantly move across domain network infrastructure, seamlessly changing between IP addresses, asset, and clouds services, tracking down malicious user activities tends to be complicated. Therefore, it is challenging to use traditional or static access control and monitoring mechanisms for authorized entities.

Here are the benefits of UBA that focus on user activities by connecting the specific user to the network, actions are contrary to traditional access control mechanism or security information and event management (SIEM) that map user to IP address or an asset and make it easier for tracking any malicious behavior earlier to an attack that then used for threat intelligence and monitoring to enforce pre-emptive control measures.

[55] Further emphasized that monitoring and identifying threats through behavior analytics considers both internal and external users. That might masquerade and infiltrate the corporate network due to compromised legitimate users to conducted malicious activities that might go undetected. Summarized functioning concept [55], "Behavior analytics deviate from traditional consumer behavioral analytics to focus on the behavior of systems and the user accounts on them." This Service is provided as part of [55] Cloud SIEM solution "InsightIDR" that unifies "SIEM, UBA, ABA, and EDR capabilities with your existing network and security stack to provide real-time visibility and incident detection across your network, endpoints, and cloud services. Behavior analytics is quite a new research world. A possible area of research is observed IoT energy conservation of the interconnected node when integrated with adaptive solution decision-making mechanism as a trust-based solution.

Chapter 3

Literature Review

This part of the document presents a systematic literature review (SLR) that identifies, selects, and critically appraises the research topic to answer the formulated question [56] based on the eight steps of [57]. A guide to conducting a standalone systematic literature review.

1. Identify the purpose.
2. Draft protocol and train the team.
3. Apply practical screen.
4. Search for literature
5. Extract data.
6. Appraise quality.
7. Synthesize studies.
8. Write the review.

According to [58], the data collection and analysis stage is crucial in determining the overall reliability and validity of the research process. Also considered to be dependent on the methodological approach adapted [59]. The listed articles and journals were analyzed by reviewing the abstract, introduction, summary, or conclusion relating to the research topic and question. Furthermore, selects the relevant ones based on Qualitative, Systematic, and Thematic review methods to build the literature review matrix and further used to facilitate Evaluation and critical review of how well adaptive security with integrated trust security based on entity behavior or reputation can be used as a risk mitigation solution for SaaS computing threat and risk.

3.1 Literature Review Data Collection

The data collection was primarily based on Secondary Data, described by [60] as data that has already been created or opinions of other researchers or intuition and organizations. This provides the groundwork for data analysis and the literature review.

The research topic data collection started by harvesting information from cloud computing scientific articles and journals via Google Scholar, Mendeley and Science direct. Further, used as

a pivoting point to the source of publications with the further growth of references list to find other articles. Search methods used were based on:

- The theme of the topic.
- Numbers of citation counts; higher the counts, the more reliable the source was.
- Relevance of the publication to the topic
- Date of publication of the articles and journals

The search parameters used on Google scholar and Mendeley were: "cloud computing" and" adaptive security."

- "cloud computing" and "risk mitigation," and "adaptive security framework"
- "cloud computing" and "risk mitigation," and "trust-based security"

Harvested information was logged, cataloged, and synthesized, as shown in Tables 1 and 2.

Table 1: log, catalog, and synthesized Research Topic Journals and Articles

Table 1: log, catalog, and synthesized Research Topic Journals and Articles		
Search Theme	Source of Literature	
	Google Scholar	Science direct
Cloud Computing	60,700	13,703
Challenges of Business Continuity Plan and Cloud Computing	39,800	1,293
Security risks in cloud computing	500	221
A Survey on Security Issues in Cloud computing	383.000	1,270

Table 2: Literature Review Matrix for Adaptive Security Risk Mitigation

Article /Journal	Author	Year of Publication	Theme	Focus	Observation
IEEE 31st International Conference on Advanced Information Networking and	M. Medhioub, M. Hamdi and T. Kim	2017	Cloud computing Adaptive Security	Adaptive Risk Management Framework for Cloud Computing	Emphases on implementing a dynamical risk treatment framework over a statically approach balance between the security and performance degradation.
Applications (AINA)					Due to the implementation of security mechanism but fall short of applying this approach to the context-based scenario.
IEEE Annual Consumer Communication ns & Networking Conference (CCNC)	M. Medhioub, T. Kim and M. Hamdi	2017	Adaptive risk treatment	Adaptive risk treatment for cloud computing based on Markovian game	Emphases on implementing dynamic security policies that will adapt to the dynamic nature of the cloud environment based on game theory modeling to weight the cost of security implementation from adaptive risk treatment. This approach was not found on the risk management procedure approach.

Indian Journal of Science and Technology	G. Jagadamba and B. Sathish Babu	2016	Adaptive Security Schemes	Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment	The author outlined the need for a dynamic context-based adaptive security for Ubiquitous healthcare, U-learning, U-smart campus, etc. over traditional static risk mitigation approach. The main mitigation focus is on security issues like access control and authentication-related risk.
Springer Nature Switzerland AG	Aman W.	2016	Context Adaptive Security Framework	Assessing the feasibility of adaptive security models for the Internet of things	The research focused on a framework that evaluates feasibility of adaptive risk management for (IoT) environment taking into consideration of the underlining architectural aspect
The Thirteenth International Conference on Systems (ICONS)	Tewfiq ElMaliki, Nabil Abdennadher and Mohamed Nizar Bouchedakh	2018	Adaptive Security in Cloud	Adaptive Security in Cloud and Edge Networks, New IoT Security Approach	The research was tailored towards adapting security framework for the IoT environment as an efficient edge-cloud security deployment, capable of trading off between security and Performance in line with (M. Medhioub, T. Kim, and M. Hamdi, 2017) research work.

International Journal of Innovative Technology and Exploring Engineering (IJITEE)	Vytarani Mathane, P V Lakshmi	2019	Adaptive Security Framework	Adaptive Security Framework for the Blockchain on IoT	The approach of adaptive security applicability to dynamic resource computation algorithm based on network existing network resources determine which security service to offer
Computer Science Review	Rakesh Kumar, Rinkaj Goyal	2019	cloud security	On cloud security requirements, threats, vulnerabilities and countermeasures: A survey	A well written detailed research survey outlining the major vulnerability, threats', and countermeasure in the cloud environment and set the trend for future research for trust adaptive security as the appropriate mitigation solution for For evolving threats in a dynamic cloud environment.
International Journal of u- and e-Service, Science and Technology	Raed Abbasi, Mohamed Hamdi and Tai-Hoon Kim	2015	Adaptive Approaches to Risk Management	Quantitative Risk Management: a Survey of Adaptive Approaches to Risk Management for Information and Communication Systems	The author of the research survey specifically emphasizes how qualitative risk assessment fits into the implementation of adaptive security mechanism. But falls short of the development of an adaptive security the framework which might not focus on the research

Elsevier Government Information Quarterly	Omar Alia, Anup Shrestha, Akemi Chatfield, Peter Murray	2020	Cloud Security Risk Assessment	Assessing Information security risks in the cloud: A case study of Australian local government authorities	The proposition of conceptual cloud computing security requirements models concerning data security; risk assessment; legal & compliance requirements; and business & technical requirements was to ensure and promote a balanced view of cloud security for the Australian government. This proposal was observed to be a traditional risk management approach.
Computers & Security	Olusola Akinrolabu, Jason R.C. Nurse, Andrew Martina, Steve New	2019	Cloud Security Risk Assessment	Cyber risk assessment in cloud provider environments: Current models and future needs	The authors set the foundation for further research work for risk inherited in de defined supply chain. First, it analyses the traditional risk assessment model to describe a new risk assessment model (CSCCRA) and compares this against established approaches.

Table 3: Literature Review Matrix for User Behavior Trust Modelling

Article /Journal	Author	Year of Publication	Theme	Focus	Observation
Epics Series in Computing	Maryam Alruwaythi, Krishna Kambampaty, and Kendall E. Nygard	2020	User Behavior and Trust Evaluation in Cloud Computing	Evaluating user behavior in the cloud environment concerning user trust level	The author's article outlined how user behavior be used to ensure a secure cloud environment. The author detailed the trust model principles and corresponding research work on different trust models' users were covered, and each significance to integrating trust modeling into cloud computing
International Conference on Instrumentation and Measurement, Computer, Communication, and Control (IMCCC)	Jun-Jian, L., & Li-Qin, T.	2015	User's Behavior Trust Evaluate Algorithm Based on Cloud Model	Evaluating user behavior based on the combination of entropy with objective weight and AHP to determine a user trust level	The authors balanced the combination of accurate weight and AHP to calculate the trust level of users with regards to how many resources were consumed. The high rate of consumption is linked to the abnormal behavior of the user.

International Conference on Information Technology in Medicine and Education (ITME)	J. Ma and Y. Zhang,	2015	Research on Trusted Evaluation Method of User Behavior Based on AHP Algorithm,	Evaluating user behavior based on expiration of trust record to determine a user trust level	The author evaluation of user behavior was based on assessing the expiration of the trust record, which are categorized into three categories; Negative range that implies far from the current time and not to is included in the trust calculation, Positive range indicates recent behavior and is applicable in the trust calculation; lastly, Uncertain range implies the record has a predictable or uncertain weight which might not be helpful in the trust calculation.
International Conference on Software and Computer Applications-ICSCA	Yang, Ruilan, and Xuejun Yu.	2017	Research on Way of Evaluating Cloud End User Behaviors Credibility Based on the Methodology of Multilevel Fuzzy Comprehensive Evaluation	Evaluation of user behavior based on the combination of AHP method and fuzzy comprehensive Evaluation to determine the user trust level	They applied various analytical hierarchical processes (AHP) with thorough Fuzzy Evaluation (FCE) to access the time impact principles. That is the number of time users spends on the cloud to determine the user trust level.
Asian Journal of Information Technology	Jaiganesh, M., et al	2016	Neuro-Fuzzy ART-Based User Behavior Trust in Cloud Computing	Evaluation of user behavior trust level based on Fuzzy Adaptive Resonance Theory (ART) and Neuro-Fuzzy Techniques	The methods compute user trust levels by assigning to what extent a virtualized client makes users of virtualized resources of Memory, CPU, GELOP, and Disk Space. The model then classifies each user as secure, vulnerable, modified, and anomaly-

					based on the usage of the resources.
International Journal of Distributed Sensor Networks	Chen, Zhenguo, et al.	2018	Trust Evaluation Model of Cloud User Based on Behavior Data	Evaluation of user behavior trust level based on both recent, historical, and recommended user behavior records.	The author determines users' trust level, modeling the behavior from the user's recent, historical, and recommended user behavior records. The outcome value is the total trust value, a combination of historical, direct, and guided trust with a weighted value as a trust factor.

3.2 Literature Review Data Content Analysis

3.2.1 Traditional Security Mitigation or Countermeasures

According to [13] [61], major information security institutions did propose recognized mitigation standards and practices. The suggested solution includes identity and access management, encryption, digital signature, message digest, intrusion detection & prevention system, web applications, and software development security measures. However, all the mentioned mechanisms were statically technical-oriented. Coupled with several recognized frameworks from ISO/IEC 27017:2015 [29], NIST Special Publication 500-291, System and Organization Controls (SOC) Reporting, General Data Protection Regulation (GDPR), CSA - Security Guidance for Critical Areas of Focus in Cloud Computing, etc. were not sufficient in tackling emerging threats.

Cloud entity and access control mechanisms, for example, Identity and Access Management (IAM), Identity-as-a-Service (IDaaS), and Cloud Identity Management were still built around the core access control principles according to [23] [45]. As a result, SECaaS proposed enhanced guidelines for IAM, and to include the following components; identity management, entitlement, authentication, authorization; Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), Discretionary access control (DAC), Mandatory access control (MAC), Rule-Based Access Control, separation of duties, Need to Know, and Least Privilege principles.

3.2.2 Adaptive Security with Trust-Context (User Behavior) for a Secure Cloud Computing

Past research has found that traditional risk mitigation solutions proposed to the Australian government concerning data security, risk assessment; legal & compliance requirements; and business & technical requirements [62] are insufficient to deal with the threat. Many researchers have emphasized implementing adaptive security mechanisms as the best way to deal with this limitation. Emphases on implementing a dynamical risk treatment framework over a static approach to balance security and performance degradation [63]. Furthermore, significant contributions for implementing dynamic security policies for the cloud environment were applied through the game theory modeling. Game theory modeling weighs the cost of security implementation from adaptive risk treatment [63]. Adapting security framework for the IoT environment as an efficient edge cloud [10]. The author points out that the mitigation can be adapted in any dynamic resource computation environment based on existing network resources to determine which security service to offer [12]. Although [12] [63] tends to coincide with this approach; however, a clear indication of how well this will fit into SaaS was not clear. Nevertheless, it still falls short of being considered as a trusted mitigation solution despite its context-based approach, and this fact is has led to further need for more research on this field, sighting trusted adaptive security as the appropriate mitigation solution for evolving threats in a dynamic cloud environment[61]. [64] one of his research works, *Risk-Based Adaptive Security for Smart IoT in eHealth*, did emphasize the need for an innovative risk-based adaptive security framework for IoT in eHealth. That will learn to identify or unknown risk, estimate and predict its damages and take the proper countermeasures to reduce risk to a minimum level. It calls attention to research on trusted adaptive security. A combination of Context and Trust-based security as a mitigation solution for the Ubiquitous Computing Environment will ensure a secure environment.

While [65] detailed the significance of trust-based adaptive security concerning Smart Grid electrical power system components interactions, [66] expressed the need to integrate this trust context in adaptive security mechanisms to ensure accurate proof of user and systems entities as indicators. They also claim many researchers classify trust into warranties and indicators and further explain proofs as certified Information (identity, property, and authorization) issued by the certification authority. In contrast, indicators are factors stored internally or externally collected from various sources. The critical component then forms the input parameters for trust-evaluation. Although these facts were relevant to the study, the researcher [67] signified that the best means of trust-based security mechanism into cloud integration should be through the following five categories*;* Reputation-based, SLA verification-based, transparency mechanism, trust as a service, and formal accreditation, audit, and standards. [68] proposed application of adaptive security decision in the presence of security threats among nodes and adapt consequently cryptographic mechanism to reduce substantial energy consumption. At the same

time, it remains secure based on trust model management for interconnected IoT systems. The section contents were extracted from Table 2 Literature Review Matrix for Adaptive Security Risk Mitigation.

Most of the research work mentioned earlier has a common drawback; they all paid less attention to user behavior trust context. Therefore, it is necessary to detail other major work that suggested the benefit of integrating user behavior trust context into an adaptive environment. The author [69] did express the significance of user trust in securing a cloud environment. [70] research work projected an effective mechanism by combining entropy with objective weight and AHP to determine a user trust level from the number of cloud resources consumed. The excessive rate of consumption of the cloud resources was then associated with the abnormal behavior of the user. [70] model fell short for not considering the user's recent behavior and repeated abnormal changes. To overcome the limitation, [71] research on “Trusted Evaluation Method of User Behavior Based on AHP Algorithm” was suggested, the evaluation of user behavior was based on assessing the expiration of the trust record, which are then categorized into three categories; Negative range that implies far from the current time and not to is included in the trust calculation as, Positive range indicates recent behavior and is applicable in the trust calculation; lastly, uncertain range implies the record has a non-predictable or unsteady weight which might not be helpful in the trust calculation. [69] also mentioned some drawbacks as it fails to evaluate repeated abnormal behavior. [72-73] both types of research were based on utilizing the Fuzzy comprehensive evaluation process. [91] applied various analytical hierarchical techniques (AHP) with thorough Fuzzy Evaluation (FCE) to assess the time impact principles. That is the number of time users spend on the cloud to determine the user trust level.[73] further, evaluate user behavior trust level based on Fuzzy Adaptive Resonance Theory (ART) and Neuro-Fuzzy Techniques. These methods compute user trust levels by assessing the extent to which a virtualized client uses the virtualized resources such as Memory, CPU, GELOP, and Disk Space usage. The model then classifies each user as secure, vulnerable, modified, and anomaly-based on resource consumption. Both [72- 73] trust models showed some limitations for not considering critical aspects of the "the principle for evaluating user behavior.”

Research work by [74] tends to be a suitable trust model that was applauded by the research community. [74] The trust model assesses a user trust based on the user behavior data on how the cloud was utilized. It covered almost all aspects of the principle for evaluating user behavior presented by [69]. [74] trust evaluation model underpinned the design part of my project work, “user behavior trust model.” The section contents were extracted from Table 3 Literature Review Matrix for User Behavior Trust Modelling.

Ultimately, researcher [75] did combine the above concept in the research work published in 2012, titled *Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security*. A combination of user behavior trust levels was derived from Neuro-fuzzy systems, which is then used as an input to generate or establish an adaptive security policy based on the user trust level.

3.3 Related Research Work

Notable and closest related work was conducted in 2012 by [75]—*Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security*. The user behavior trust evaluation was based on the Neuro-fuzzy systems. Information about the user behavior in trust contexts was recorded and fed into the Neuro-fuzzy systems to evaluate and generate trust. The Neuro-fuzzy mechanism continuously evaluates the trust level and updates its internal database. The estimated trust level is then used as a parameter to establish an adaptive security policy. Finally, the security policy is established by the adaptive security system based on the user behavior trust level fed as an input parameter.

Due to insufficient research work and articles published by the research community regarding integrating user behavior trust context into policy decision making and adaptive security solutions. Based on the under-develop area of this research, the goal of enhancing user identity and access control across SaaS environments has prompted my project work to draw up and rely on additional previous works and articles tailored within the field of IoT. Trust context with adaptive security within the IoT field of studies where known to be significant for IoT hosts energy conservation. In the IoT field of studies, trust-based adaptive security solutions eventually enhanced energy consumption reduction and security management for interconnected nodes. Based on these facts, the IoT research field and [75] research work will become relevant to transform this idea and working principles into the SaaS environment and eventually form my project's basis.

[12] The proposed adaptive security framework for IoT blockchain architecture as a dynamic resource computation algorithm for nodes on the blockchain did ensure adequate resource management and decide which security services to offer. This mechanism helps overcome the lack of support in managing different network resources and powering interconnected IoT devices. While[76]publication addresses Mobile crowdsensing, crowdsourcing of sensor data from mobile devices that support the production and sharing of data across the IoT applications by proposing a reputation-based security framework to evaluate sensor devices based on reputation score using the Bayes algorithm. [68] Research focuses on deriving an adaptive solution for reducing energy consumption during cryptographic processing for Internet of Things (IoT) communication in a dynamic low-power environment while still maintaining security. Furthermore, [7] addresses the issues of processing capabilities, resources usage, and risk across the IoT eHealth platform while ensuring security and privacy by proposing a *Risk-Based Adaptive Security for Smart IoT in eHealth* framework using game theory context-awareness technique. [28] derived a User Trust Model for a Smart environment that will positively influence users' experience and acceptance of the intelligent system. Also noted was that intelligent energy consumption saving mechanism, when put in place to reduce energy consumption, might affect the proper functioning of these smart systems during operation, such; as light, display, and

brightness in-room or presence of users. Lastly, research work by [54] also emphasizes trust-based decision-making for smart energy systems and adaptive environments.

As a result of the above successful adaptation of the IoT solution, backed with several research findings in an IoT environment, it is possible to conclude that adaptive security, when integrated with user behavior trust context and policy decision point, could be a way forward—ensuring better mitigation against identified or unknown threats when operating in a dynamic environment like the SaaS public cloud.

3.4 The Research Gap and Justification of this Research

Related research work conducted in 2012 by [75] was tailored towards user behavior trust-based adaptive security policy, which was fine. Still, there is a need to adopt a similar concept to cloud computing user identity and access control with the risk management process; the idea forms the underpinning work of my research.

Furthermore, [7],[12], [16], [28],[68], and [76] emphasizes adapting trust-based context into adaptive security as a significant shift from the traditional static mitigation method for managing threats risk across ubiquitous computing environments such as the cloud environment and IoT. However, their research fell short of integrating user behavior trust context with adaptive security into the risk assessment process that could help enhance user identity and access control mechanisms across cloud computing.

Coupling the above facts mentioned earlier eventually formed the basis of my research aim and objective, inducing the research initiative to design a risk mitigation solution that might be applied as a risk treatment within ISO/2705:2018 process[29]. The goal is to secure the SaaS computing environment regarding the safety of users and how their access granted is managed.

The justification of this research is based on the need to integrate user behavior trust context with adaptive security solutions and policy decision making as a mitigation solution within the risk management process that would help enhance identification and management of cloud users' access across the SaaS environment. The idea came as a result of interest and studies from the following research work ;

- *Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security* conducted in 2012 by [75] was tailored towards user behavior trust-based adaptive security policy,
- *Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment: A Comprehensive Survey* [9][16] a survey research study. The need to develop a Trust-Based Adaptive Security Framework as an add-on to this work will

support the risk management's mitigation process to ensure a secure SaaS computing environment against emerging threats.

- Most of the research on trust and adaptive security mentioned in the" Related Research Work " section was exclusively tailored towards the Internet of Things' energy consumption conservation while securing the IoT system; precisely from the following list of research work on IoT; *Risk-Based Adaptive Security for Smart IoT in eHealth* [7], *Adaptive Security Framework for the Blockchain on IoT* [12], *Trust-based decision-making for smart and adaptive environments*[28] [54], *TAS-IoT: Trust-Based Adaptive Security in the IoT* [68] and *Reputation-Based Security Framework for Internet of Things*[76]. The applicability of this concept or solutions has shown success in conducting a risk assessment for eHealth, cryptographic processing, Smart energy systems, Blockchain energy consumption management, and a risk countermeasure.

Applying a similar idea and approach to the SaaS environment for risk treatment will be highly significant. In addition, the project might probably form the foundation for further research to improve a trust-based adaptive security framework as a mitigation solution for a secure SaaS environment. Specifically when dealing with adequately identifying entities (user and process) and their associated access management.

Chapter 4
Methodology

4.1 The Proposed Methodology Research Method

As defined by [58], a research design methodology is a systematic design method or approach applied by researchers to address research aims and objectives to produce a possible valid result in answering the research question. The widely accepted practical design step by [59] will be the foundation for designing a methodology to address the research problem explained later in subsequent sections. The research approach follows a broadly deductive and qualitative design approach. The deductive approach develops hypotheses from pre-existing theories to test a theory [77]. The qualitative approach allows interpreting something and focuses on words and meanings. In other words, it focuses on textual, visual, or audio-based data. Since inductive methods are usually used within qualitative research, updating a mixture of both approaches will be suitable for data collection and transforming this data into the theory that aligns with the research aim and objectives. On the other hand, quantitative methods focus exclusively on numbers and statistics and are unsuitable for the research question.

To archive, the aim of answering the research question, *"*How can a trust-based adaptive security framework be integrated into risk mitigation to enhance SaaS user- identity and access control based on user behavior?". The solution will be developed and designed as a security solution in Phase 1: Framework Design: *Trust-Based Adaptive Security Framework based on User Behavior* and then integrated into Phase 2: Implementing: *Trust-Based Adaptive Security Framework based on User Behavior* as a risk treatment for SaaS user identity and access control management within risk management process. ISO/2705:2018. ISO/2705:2018 process is a well-established standard used in the information security field of practice and fits the research methodology's purpose. Therefore, the procedure will follow the ISO/IEC 2705:2018 guideline, shown in figure 1.

4.1.1 Phase 1 Design: Trust-Based Adaptive Security Framework based on User Behavior.

The *Trust-Based Adaptive Security Framework based on User Behavior* will be designed and underpinned by the following three significant scientific research and models; User Behavior Evaluation Model from *Trust evaluation model of cloud user based on behavior data* scientific

research work by [74], *Gartner Adaptive Security Architecture Model* [78] and *eXtensible Access Control Markup Language's policy decision point* concept[79]. The design components will consist of and function as follows:

The User Behavior Trust Manager:- A system built around the "Seven principles for evaluating user behavior," the fundamental principle underpinning user behavior evaluation. A Behavior Trust Evidence Collection; is the log collector; it collects information from different computing systems that are log sources. The collected logs information consists of cloud user activities before and after access is granted across the cloud. The data is then used to derive the user behavior pattern. Secondly, Behavior Data Analysis; evaluates the collected user logs data, which is then correlated, indexed, and analyzed to create a user behavior trust profile that is later used to determine the users' trust state and risk rating. Thirdly, trust evaluation- The Computation Engine does the user behavior evaluation and computation of three different types of trust; Direct Trust, Recommendation Trust, and Historical Trust. These three types of trust are then computed with a weighted value to derive the overall trust level of the user behavior, known as the Comprehensive Trust Degree. The comprehensive trust degree value will feed the Policy Decision Point. The comprehensive trust degree value will also update the historical and user behavior trust lists.

Policy Decision Point (PDP) Central Server:- The idea of integrating the policy decision point server as part of the solution came from the specification standard for eXtensible Access Control Markup Language. It defines the declarative fine grinned access control policy-based attribute and evaluates access requests based on rules defined within the policies [79]. The policy decision point server processes the feeds; user behavior comprehensive trust degree and user behavior risk rating received as input from the trust managers database. It will process this input through logical processing to make an authorization access control decision. The adaptive security engine will then use this outcome to enforce the corresponding security controls depending on the user behavior and risk rating.

Adaptive Security Control Engine:- this system will function as a security control enforcement point that allows, limits, or denies cloud users access depending on the outcome decision received as input from the policy decision point. Decision-making and enforcement of corresponding controls will be influenced by the user behavior, trust level, and risk rating. Depending on the type of decision made by the policy decision point for a user behavior trust level and associated risk rating, the adaptive security solution will perform any or combination of the following controls; Preventive Capabilities, Detect Response/Retrospective Capabilities or Predictive Capabilities.

4.1.2 Phase 2 Implementation: Trust-Based Adaptive Security Framework based on User Behavior. As Risk Mitigation Solution in Risk Management process ISO/2705:2018.

Context Establishment covers:

- Information Assets and Scope gathering information of SaaS user as people asset
- The Risk Management approach is based on the ISO/IEC 27005:2018 procedure outlined in figure xxx above.
- Establish Risk Appetite and Tolerance Declaration statements for Risk Appetite, Risk Tolerance, and Risk Threshold
- Risk Evaluation criteria will be criteria's Risk Appetite, Risk Tolerance, and Risk Threshold were used to compare each identified risk exposure and residual risk to see if they are acceptable or require further assessment and treatment.
- Risk Estimation Will be a Qualitative approach on Impact criteria and threat likelihood to determine risk exposure.
- Impact criteria were developed in terms of the extent of degree of damages caused by compromise of any of the CIAA objective, Reputational Damages, Regulatory Implications, Legal Implications, Financial Loss
- Risk acceptance criteria This is associated with Risk Evaluation criteria Risk Appetite, Risk Tolerance, and Risk Threshold

Risk Analysis covers:

- Risk Identification centered around user and process entity for SaaS system utilization.
- SaaS applications or critical, vulnerability and threats
- Risk Estimation; Qualitative approach
- Risk Evaluation based on Risk Appetite, Risk Tolerance and Risk Threshold derived from declaration statements
- Risk Treatment Implement "*Trust-Based Adaptive Security Framework based on User Behavior.*"
- Risk Acceptance Evaluation: Risk acceptance criteria derived from Risk Appetite statement and Risk Tolerance Statement

4.2 Motivation for Methodology Selection

One of the key motivating factors for selecting the methodology is the interest in user behavior trust context [74] concerning cloud-computing resource utilization and resulting risk from their actions. How the users' trust is evaluated based on their activities and behavior, afterward integrates this trust level into the policy decision-making process, adaptive security system to produce dynamic security controls[78], could be pretty interesting to apply this concept to the SaaS environment concerning to user and access management. As a result, the end goal is to

design an adaptive trust-based security architecture within the context of user behavior and policy decision-making that could help improve how cloud users can be identified and their granted access managed adequately within a dynamic environment.

Another motivation factor is adapting the ISO/IEC 2705:2018 procedure for risk assessment and treatment for identified risk from user behavior trust level and risk ratings across the cloud. The application follows the standard risk management process guideline in the information security field of practice. Therefore, adhere to the standard way of conducting the risk management process in answering the research question. Although, there are other standard guidelines available for risk management like NIST, OCTAVE Allegro, and ISO/IEC 27017. But the purpose of my research is to integrate the proposed framework within the ISO/IEC 2705:2018 process to provide a possible general guideline for cloud service providers and cloud service customers and form the bases for further research within the research community. In addition to the above reasons, l considered the choice of methodology based on ISO/IEC 2705:2018 to be best suited in conducting step by step risk assessment and treatment over other guidelines due to its worldwide acceptance with a proven record of widely adapted and flexibility into any information security filed of practice, including cloud computing.

The focus of my research is about building a risk mitigation framework to answer the research question; “How can a trust-based adaptive security framework be integrated into risk mitigation to enhance SaaS user- identity and access control based on user behavior*?”*

Chapter 5
Design and Implementation

5.1 Phase 1 Design: Trust-Based Adaptive Security Framework based on User Behavior

5.1.1 High-Level System Design Presentation

The overall system design of the *Trust-Based Adaptive Security Framework based on User Behavior* is presented in figure 17 and serves as a risk mitigation solution. The essence of the solution is to provide a possible guideline in establishing a hierarchical access control between the user and SaaS resources. Through crucial capabilities of; user-behavior trust evaluation model, policy decision point, and adaptive security control processors. As presented in figure 17, adaptive security processors function as a policy enforcement point that adjusts the access request permissions dynamically, according to inputs fed indirectly from the trust evaluation model through the policy decision point server. Policy decision point server performs a logical processing on trust level and associated risk rating received directly from trust evaluation model. These inputs then determine if to allow, limit, or deny the user access request. Subsequently, it signals the adaptive security processors to dynamically adapt and enforce the appropriate control decision.

The significant advantage of the solution is its ability to provide a hierarchical access control strategy for SaaS cloud resources access and utilization. Additional systems are also presented in figure 17, the RBAC, which provides an authorization mechanism as a second-level security control. At the same time, the identity provider´s IAM or IDaas does authentication at the first level of control. Lastly, the adaptive security control engine implements the third security control level across the cloud, based on the user-behavior trust level.

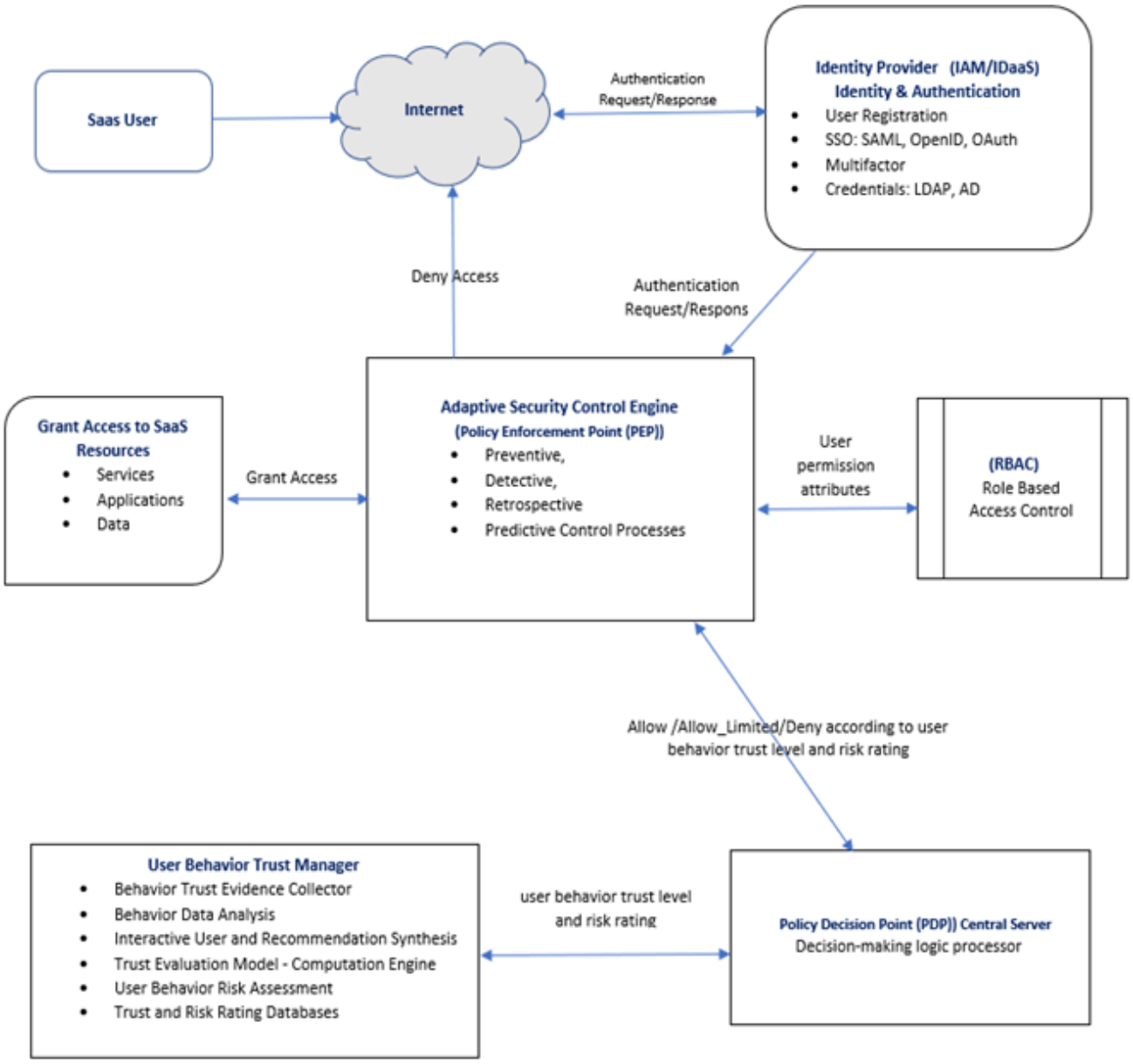


Figure 17: The High-level system design & access control process

5.1.2 Low-Level System Design Presentation and Operational Functionality

- **User Initiate Access Request**

The low-level system design presented in figures 18, 19, and 20 detailed the key components and functionality that collectively produce the dynamic hierarchical access controls capability. The access control process starts when users initiate an access request to any hosted resources, such

as; Microsoft Office 365, Box, Google Apps, Amazon Web Services, Concur, Zendesk, DocuSign, and Data. The cloud identity provider intercepts this request to initiate an authentication process. Depending on the authentication mechanism, the user is subjected to identity verification and authentication through any of the following means; SSO: SAML, OpenID, OAuth, Multifactor or Credentials: LDAP, Active directory services. If successful, user role authorization assessments are activated; on the contrary, the user is denied access and feedback sent to the user. This process is the first layer of the access control process.

- **Adaptive Security Control Engine (***Policy Enforcement Point (PEP))*

The adaptive security control engine shown in Figure 18 is the heart of the access control process enforcement. Successfully authenticated users are further subjected to the second level of the access control process by consulting the RBAC, role-based authorization server. The role-based authorization server defined the authorization criteria based on user identity, associated roles, and permission within an access control matrix or capability tables. A capability table is one method of identifying privileges assigned to the subject (user, groups, or roles), focusing on the subjects, and identifying the objects that subjects can access. [80]. A user granted access is subjected to behavior observation and analysis by the User Behavior Trust Manager's evaluation modeling engine. The trust evaluation model assesses and assigns trust and risk rating values to each user's behavior, then feeds this into policy decision points to determine access permission. The adaptive security control engines ultimately enforce the access permission for each user accessing and utilizing the cloud resources.

The adaptive security control engines act as a particular policy enforcement point, depending on the decision feedback received from the policy decision point server. Furthermore, it monitors, predicts future risk events, and responds to security incidents associated with initially authorized user activities. Figure 18 presents the adaptive security architecture process, while the subsequent sections explain each system's capabilities in-depth.

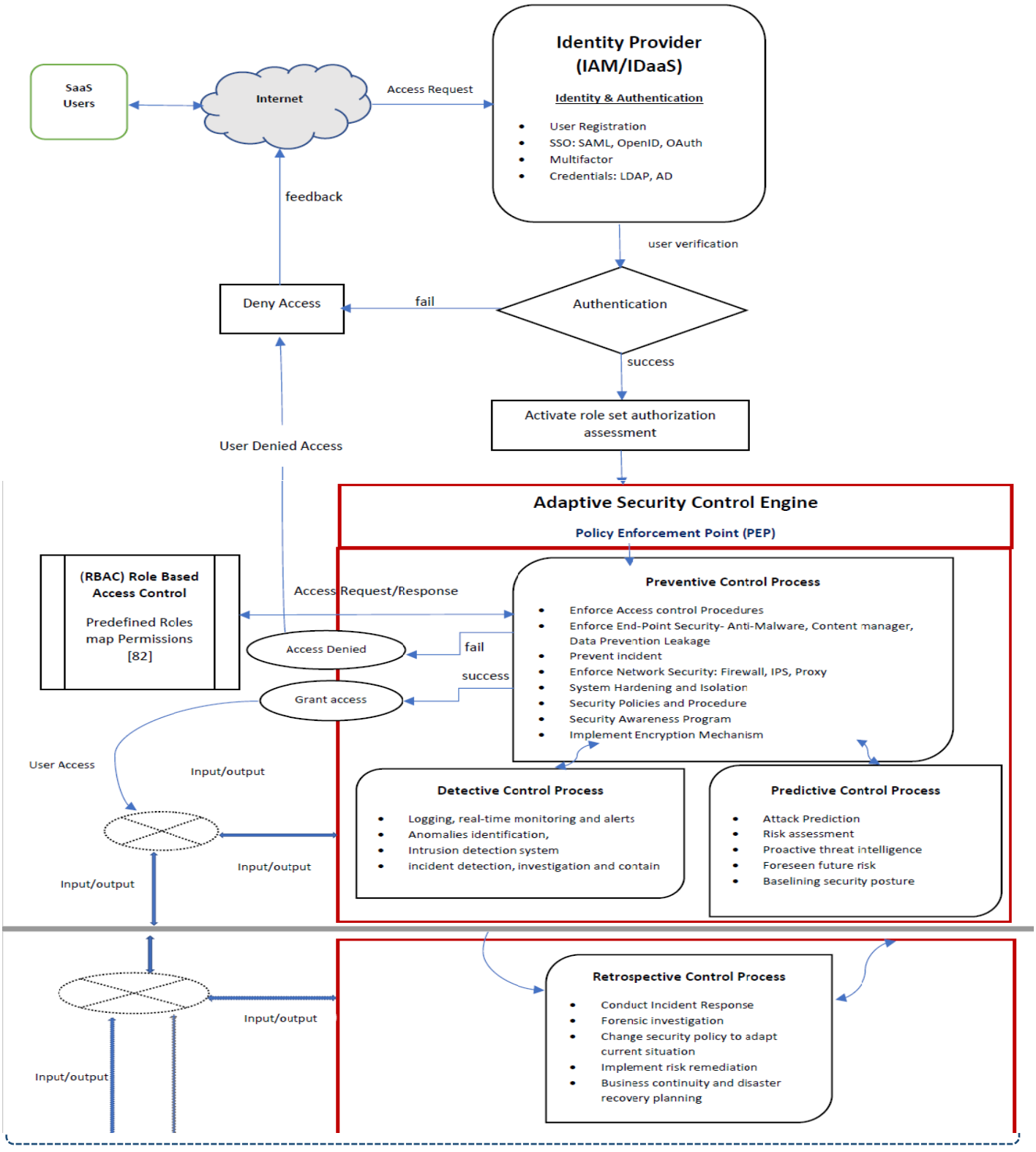


Figure 18: Process of Adaptive Security Architecture [78]

1. Preventive Capabilities -Prevents or deter undesirable events from users. For example, activities of Users' behavior with “not credible trust level and high-risk ratings” will be denied access. While users with both trust level and risk rating of “partial trust level and medium risk rating” are given “limited access” and subjected to detective and response processes in case there is further punishment by the trust model engine. The preventive feature can ultimately deny access already granted to a user due to the user's bad behavior, which seamlessly increases the user behavior risk rating. For this enforcement to happen, the preventive capability makes use of the currently updated user behavior trust level degraded to a much lower level, newly computed by the trust evaluation model.

The substantial risk that can occur without the existence of ineffective preventive controls is, for example, unauthorized information disclosure, modification, and destruction either through intentional or non-intentional threats. Applicable controls enforced at this layer, as shown in figure 18, can be; Security policy and procedures, Security Awareness Training, Access control procedures end-point security such as multi-factor authentication, consisting of signature-based anti-malware protection, network perimeter security such as application proxies, intrusion prevention systems, firewalls, and System hardening and isolation [78]

2. Detective Capabilities -Identify and provide insights into undesirable events and alerts to the system administrator. All users' activities, both “complete or limited access,” are still subjected to monitoring and detective control process if their attributes are downgraded due to misbehavior when using authorized resources. The substantial risk that can occur without the existence of ineffective detective controls can be, for example, security breaches, multiple unsuccessful attack attempts, and suspicious reconnaissance. Appropriate controls enforced at this layer, as shown in figure 18, can involve; Logging, real-time monitoring, and alerts anomalies identification, Intrusion detection, incident detection, investigation, and containment.

3. Response/Retrospective Capabilities -Intelligently and automated response actions to promptly address security incidents to minimize incurred risk events and restore processes and services to a normal state. This control engine will trigger an incident response procedure as a countermeasure in the phase of attempted or successful security breaches due to unauthorized access or abuse of privileges by users with complete trust and partial trust levels. Applicable controls enforced at this layer, as shown in figure 18, can involve, Conduct Incident Response, Forensic investigation, changing security policy to adapt current situation, Implementing risk remediation, Business continuity, and disaster recovery planning [78]

4. Predictive Capabilities -The user behavior trust levels and risk ratings can be used to evaluate and provide the possibility to foresee unwanted security events through intelligence monitoring, analytical, diagnostic to identify attacks before they materialize. Appropriate controls are enforced at this layer, as shown in figure 18, which can involve,

Attack Prediction, Risk assessment, Proactive threat intelligence, Foresee future risk, and Baselining security posture. [78]

- **Policy Decision Point (PDP) Central Server**

The idea of integrating policy decision point server as part of the solution came from specification standards for eXtensible Access Control Markup Language. The standard defines a declarative fine-grained access control policy-based-attributes and evaluates access requests based on rules defined within the policies[79]. Figures 19 illustrate the access control decision-making process from higher and lower levels perspectives. The adaptive security control engines consult the PDP for outcome authorization decisions based on user behavior's trust level and behavior risk rating to dynamically adjust and enforce the corresponding controls as presented in figure 19-a.

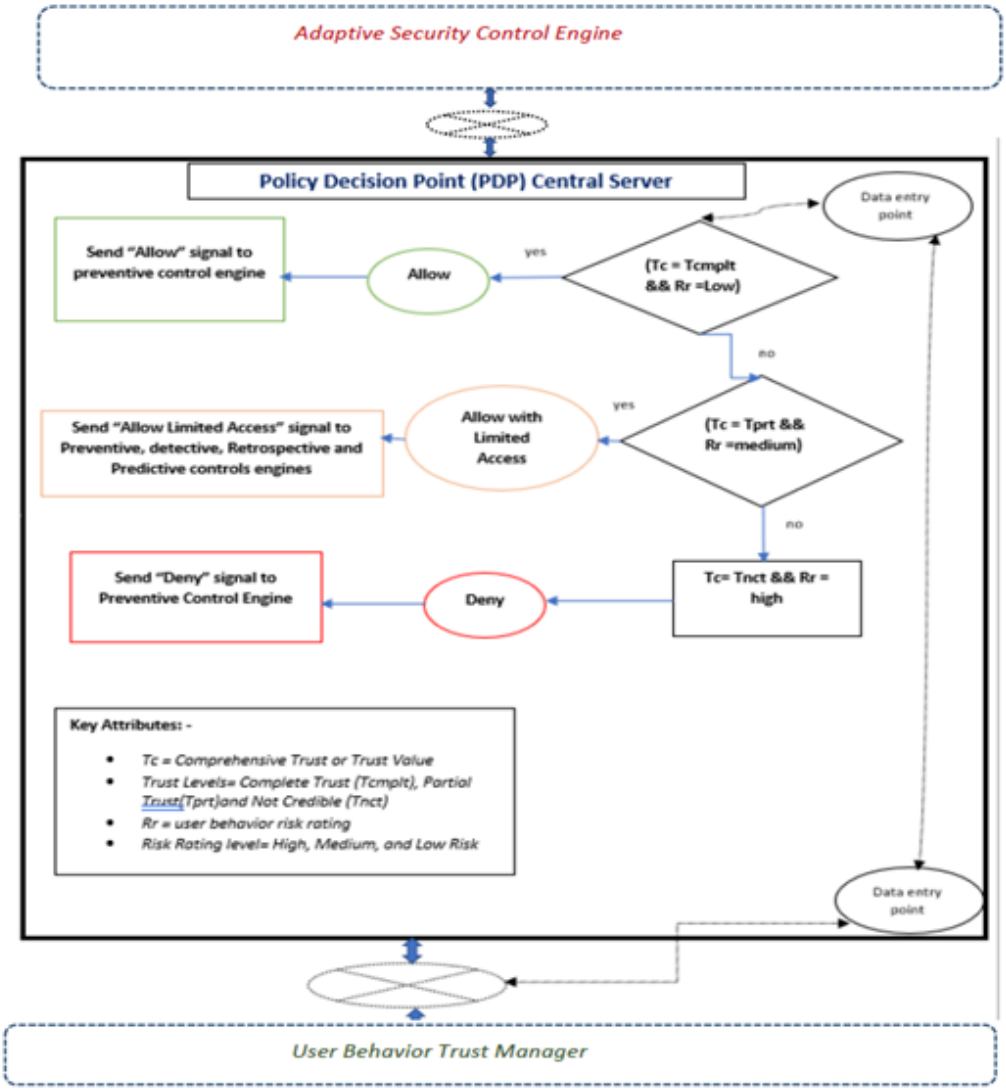


Figure 19-a. Decision-making process -User behavior trust and Risk

PDP will retrieve all user behavior comprehensive trust degree and associated risk ratings from the Trust Degree and Risk Rating Databases, integrated as part of the User Behavior Trust Manager through a data entry point to make the authorization decision. Before decision making, these parameters are adapted and categorized to suit the process. The categorized user behavior trust level comprises of; Complete Trust, Partial Trust, and Not Credible Trust, and associated behavior risk ratings of; High, Medium, and Low Risk. The logical processor presented in Figure 19-b is the brain behind the logic. First, logically process the trust and risk values to arrive at an access decision making, afterward interpreted at a high level in figure 19-a.

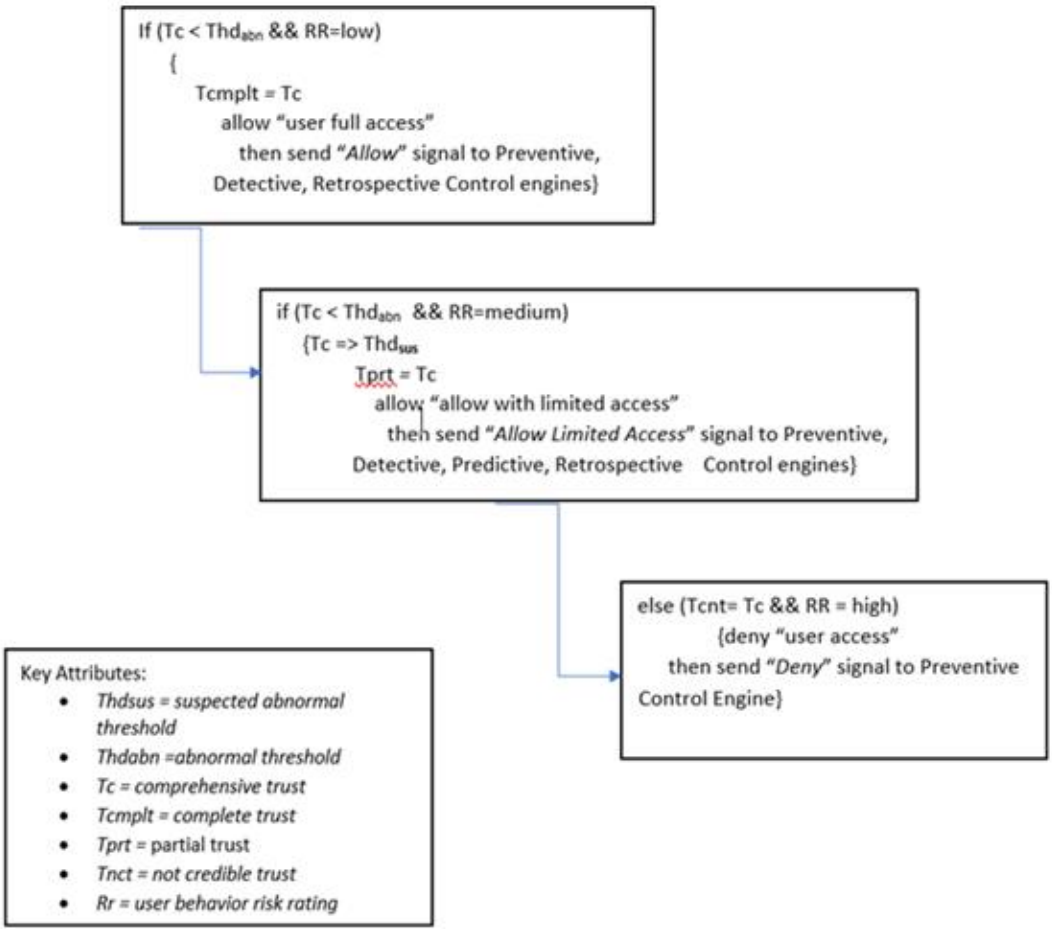


Figure 19-b. Decision-making process- Logical Processor

- **User Behavior Trust Manager System Design & Components**

As presented in figure 20, several critical components must function collectively to produce a well-functioning trust evaluation capability. These components include behavior trust evidence collector, Interactive user collector, risk assessment process, trust and risk databases, and trust evaluation modeling engine. The development of the User Behavior Trust Manager system is

drawn from research work conducted by [74] titled, *Trust evaluation model of cloud user based on behavior data.* The author [74] covered the fundamental principles "Seven principles for evaluating user behavior" required for the trust assessment.

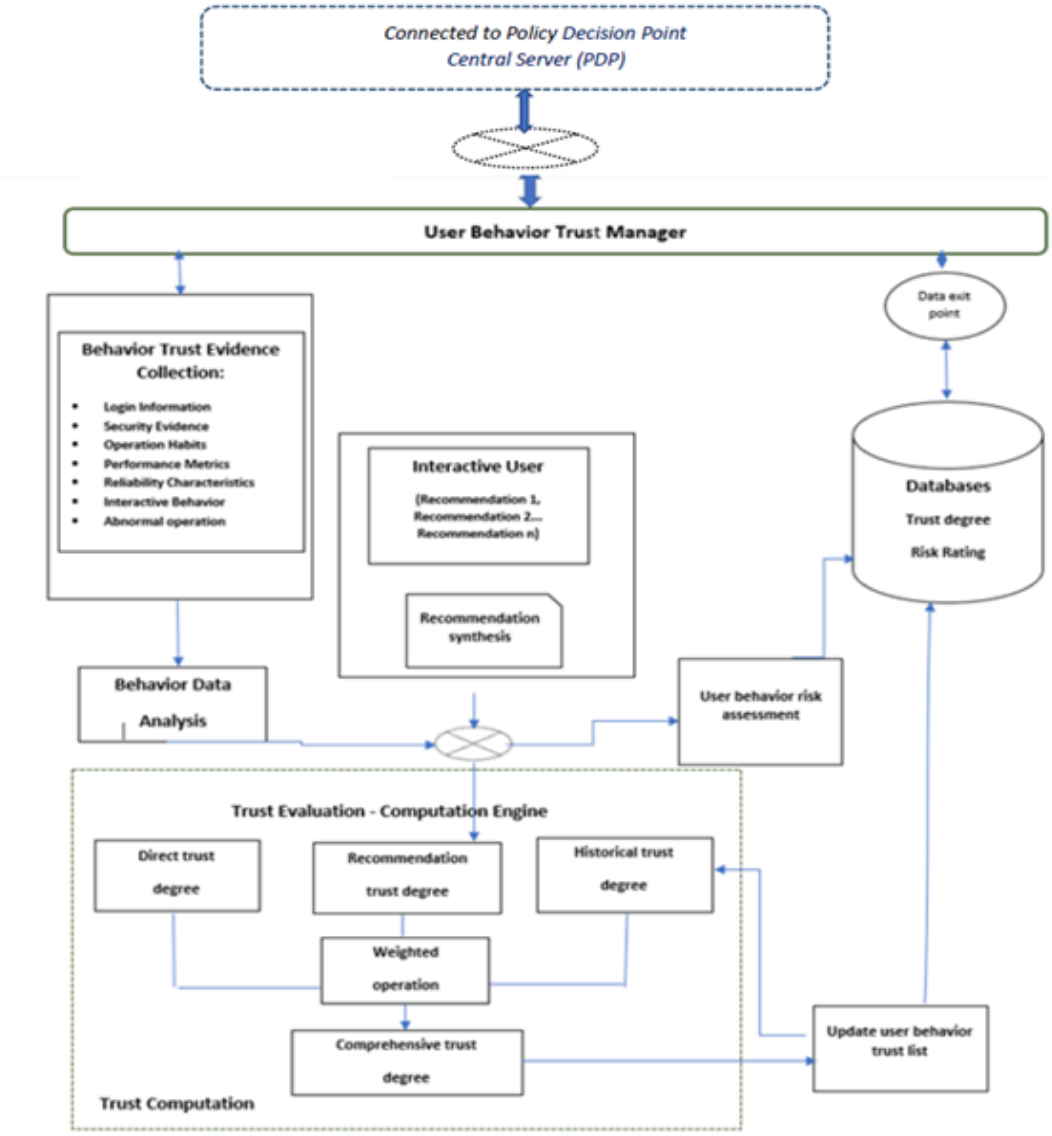


Figure 20: Process of Trust Evaluation [74]

To develop a well-functioning trust modeling that might determine the trustworthiness of users during the period when connected to SaaS resources, several principles must be taken into consideration that should include the following:

1. Seven Principles for Evaluating User Behavior [69]

- Time Impact Principle: Involves the duration of time a user stays connected to the SaaS cloud services. The seven principles are fundamental because the kind of activities carried out during the connection period might reflect the level of risk the user can impose on the cloud service.
- Expiration Trust Record: Behavior trust records that are outdated and very old are not reliable to be considered for evaluation because users stopped accessing the cloud or not recently.
- Recent User Behavior: New user behavior weighs heavily in calculating the trust value of a user. It reflects any user activities' current or new behavior when accessing the cloud.
- Abnormal Behavior: Suspicious activities and abnormal attitudes are significant when calculating trust value compared to normal behavior.
- Repeated Abnormal Behavior: Subsequent repeated behavior noticed as repeated malicious behavior is considered a key factor used in a rapid decline of trust value and punishment imposed.
- Punishment Strategy: Strategy based on the rapid decline of user trust value due to repeatable abnormal behavior.
- Trust Fraud Risk Through Slow Rise: Based on more significant numbers of users accessing the resources. The more important the number of users and available resources, the more accurate trust value evaluation. Therefore, it aims to prevent trust fraud risk during the trust evaluation process.

Based on figure 20, the subsequent sections describe the trust evaluation process, a vital User Behavior Trust Manager component. The derived user trust value and risk rating are then fed into the policy decision point server for access decision-making. Finally, the adaptive security controls engines, in turn, use these values as inputs to dynamically adjust and enforce access controls in the SaaS environment.

2. Behavior Trust Evidence Collection

This process collects evidence of users' activities across the SaaS infrastructures. These are composed of different logs types from a variety of data sources. Next, they aggregated parsed to transform the specific logs format into common structural data. Finally, the common structural data undergoes correlation and indexing, which afterward is fed into the Behavior data analysis process. As presented in figure 20, the list of standard logs types that will be required consists of:

- User Login Information (Username, IP address, geolocation, login time, logged and login domains)

- Security Evidence (security events across firewall, intrusion system, malware, unauthorized access events
- Operation Habits (file upload, download, file search, directory access, read, write, or execute an event, frequency of resource usage, abnormal operation, interactive behavior, and operational functions)
- Performance Metrics (Data request and response times, system resources occupancy rate, data transmission capacity usage)
- Reliability Characteristics (Error rate of transmission failures, rate of denied connections, rate of, rate of IP packet loss)
- The log sources can be diverse, coming from a source like; Network and End-Point security devices Logs, Application Event Logs, Network devices Logs, User Session Logs, Computer Systems Logs, Data processing, and transmission, Database Logs, Authentication and Authorization Logs, and Web Servers Logs. [69][74][81]

3. Behavior Data Analysis

The collected trust behavior evidence from different log sources are analyzed to create a user behavior trust profile that is later used to determine the users' trust state and risk levels, as shown in Figure 20. Based on [74] trust model computation, the user behavior profile can be determined by applying several mathematical formulas shown below:

Deriving Cloud User Behavior set (*CB*) from categories of user behavior:

Examples of cloud user behavior set; cb1 = user authentication, cb2 =download behavior, cb3= upload behavior, cb4= retrieval behavior. [74]

$$\boldsymbol{CB} = \{\boldsymbol{cb_i} | \boldsymbol{i} \text{ is a natural number}, \boldsymbol{and}\ 0 < \boldsymbol{i} \leq \boldsymbol{N}\}$$

i is a natural number, where N= total number of users' behavior.

Deriving Cloud User Behavior State set (CBS) from Activities performed and attitude within, from each category of user behavior set:

$$\boldsymbol{CBS} = \{\boldsymbol{cbs_j} | \boldsymbol{j}, \boldsymbol{i} \text{ is a natural number}, \boldsymbol{and}\ 0 < \boldsymbol{j} \leq \boldsymbol{m_i}, 0 < \boldsymbol{i} \leq \boldsymbol{N}\}$$

Examples of cloud user behavior state set.

*"*User authentication (Normal users and legal IP, abnormal users and legal IP)

Retrieval behavior (Retrieval method = combination search, retrieval content = some areas)

Download behavior (Download frequency = any, download mode = single download, download content = any,), download category = any

Upload behavior (Upload category = any, upload frequency = any)" [74]

Deriving Cloud user behavior Weighted value; weight assigned to each user behavior based on historical and statistical recorded data to provide credibility of the user profile. For example, the weighted value will be needed during trust computation when deriving a user's comprehensive trust degree or value. [74]

$$\varepsilon = \{\varepsilon_i | 0 < i \leq N\}$$

Deriving Cloud User Behavior Trusted State set ($CBS^{TRUSTED)}$) from a collection of regular activities and attitudes within each category of user behavior set that is deemed trusted without abnormalities.

$$\boldsymbol{CBS^{TRUSTED}} = \left\{ \left\{ \boldsymbol{cbs_j^{trusted}} \right\}^i | \boldsymbol{j, i} \right.$$
$$\left. \text{is a natural number, } \boldsymbol{and}\ 0 < \boldsymbol{j} \leq \boldsymbol{p_i}, 0 < \boldsymbol{i} \leq \boldsymbol{N} \right\}$$

Sample of the status set of trusted users:

"$CBS^{TRUSTED}$ = {{normal users and legal IP},{retrieval method = combination search, retrieval content = specific area}, {download frequency = download each time, download mode = batch download, download content = specific area, download category = pdf}, {upload category = none, upload frequency = never upload}}" [74].

4. Interactive User

Interactive user presented in figure 20 is the process of collecting information about user activities and related behavior through direct interaction with other entities; either through other cloud service providers or entities within the same domain that the evaluated user resides, is significant in building the recommendation synthesis that will be needed during the trust computation to derive recommendation trust. Therefore, an Indirect interaction with the evaluated user is not considered valid. The reason is to avoid non-credibility or reduce the size of the recommendation chain.

5. Trust Evaluation- Computation Engine

The trust evaluation engine is the heart of the User Behavior Trust Manager. As presented in figure 20, the trust computation process computes a series of trust degrees or values (direct

trust, recommendation trust, and historical trust) from data received from behavior analysis, recommendation, and historical recorded statistics. The mentioned trust types and weighted values are then fed as inputs and collectively computed to determine the overall trust value known as comprehensive trust degree. The comprehensive trust degree or value is further used to update the user behavior trust list and additionally sent to the database for storage. The following sub-sections outline how the different trust types are derived.

- Deriving Direct Trust *(T_d)*

Direct trust is derived from real-time statistical records of interaction between the user and the SaaS resources. Data collected from user behavior data analysis process consist of; Cloud user behavior set, Cloud user behavior state set, Cloud user behavior Weighted value, and Cloud user behavior trusted state set, are used by the trust computation to derive the direct trust degree based on the formula below [74]:

$$T_d = \left\lfloor MAX \times \left(\left(l \times \sum_{i=1}^{l} \varepsilon_i \right) / (1 + k) \right) \right\rfloor$$
$$0 < k \leq N, 0 \leq l \leq k$$
$$T_d \in [0, MAX]$$

Td = Direct Trust Degree

MAX is considered as a direct trust set based on historical experience.

- Deriving Recommendation Trust *(T_r)*

Recommendation trust is the trust derived from recommendations provided by direct interaction of the user evaluated with other entities or entities within the user domain at real-time interaction. Collected recommendations are synthesis to generate the recommended trust value, which is then fed as input to the trust computation. The formula below is used to derive the recommendation trust degree [74].

$$T_r = \left\lfloor \left(\sum_{i=1}^{w} (T_{ci}/w) \times \left(Inter_{success}^{inner} / Inter^{inner} \right) \right) + \left(Inter_{success}^{outer} / Inter^{outer} \right) \right\rfloor$$

Tr = Recommendation Trust Degree
Inter = Number of direct interactive requests after user login in the cloud.
$Inter^{inner}$ = Numbers of direct interactive requests to internal platform
$Inter^{inner}$= Numbers of successful direct interactive requests recorded
- *success*

$Inter^{outer}$ = Numbers of direct interactive request cross-platform
$Inter^{outer}$ = Numbers of successful direct interactive requests recorded cross-platform
- *success*

T_{ci} = comprehensive trust of the ith internal users.

- Deriving Historical Trust *(Th)*

Historical trust is the last calculated "direct trust value" influenced by historical statistics and expert experience. The historical trust is further updated according to comprehensive derived trust, suspected and abnormal thresholds. The value can be derived using the formula [74].;

$$T_h = \begin{cases} T_c, T_c < Thd_{susp} \\ T_c - |T_c - Thd_{susp}|, Thd_{\text{susp}} < T_c < Thd_{abn} \\ T_c - \tau \times |T_c - Thd_{abn}|, T_c \geq Thd_{abn} \end{cases}$$

T_h = *Historical trust*

T_C = *comprehensive trust*

Th_{us} = *suspected abnormal threshold*

Thd_{abn} =*abnormal threshold*

t = penalty coefficient and can be adjusted to intensify user behavior punishment.

- Deriving Comprehensive Trust *(Tc)*

Comprehensive trust is the overall trust value derived from the entire process. It is obtained from collectively computing the calculated weighted average, direct trust, recommendation trust, and historical trust during the trust computing process. The comprehensive trust value is used as decision-making parameters by the policy decision point server as presented in figure 19-a, *Decision-making process -user behavior trust and risk access control,* and figure 19-b, *Decision-making process-Logical Processor*. Afterward, the adaptive security control in figure 18, *Process of Adaptive Security Architecture*, ultimately does the enforcement. This value can be derived using the formula [74];

$$T_c = \lceil \alpha \times T_d + \beta \times T_r + \gamma \times T_h \rceil$$

T_C = *Comprehensive Trust*

T_h = *Historical trust*

α,β,γ = *weighting coefficients*

$0<\alpha, \beta, \gamma<1, \alpha+ \beta+ \gamma=1$.

6. User Behavior Risk Assessment

User risk assessments are performed based on the analyzed user behavior data inputs from the *Behavior Data Analysis* and *Synthesized Recommendations*. Risk Ratings are assigned to each user based on individual behavior, ranging from Low, Medium, to High. The Risk Rating values are stored in the risk rating database that the policy decision point server will consult during processing, as presented in figures 19-a and 19-b.

7. Database (Trust Value and Risk Rating Database)

Computed user behavior trust values or degree and risk ratings are stored in this database, shown in figure 20. In addition, it is interconnected to the Policy Decision Point Central Server through its data exit point to PDP's data entry point. It facilitates data communication exchange between the two systems, as presented in figures 19 -20.

5.2 Phase 2 Implementation: Trust-Based Adaptive Security Framework based on User Behavior. As Risk Treatment Solution in Risk Management Process ISO/2705:2018.

5.2.1 Context Establishment

- **Information Assets and Scope**

The information assets and scope include any organization's employees at all levels, students, and business partners as a Cloud Service Consumer. They regularly use the SaaS resources for daily business operations.

The entities are significant assets to any organization; as such, conducting risk assessment and applying the application mitigation strategy regarding individual activities and behavior is highly relevant in maintaining a secure cloud environment when using SaaS applications and data. Compromising any CIA-A security objective will be detrimental to the organization and its business partners and customers.

- **Definition of the Scope and Boundaries (Information Asset Identification and Categorization)**

Information asset identification and categorization is the process of collecting data, data set, or any asset that collects, processes, transmit, or store information valuable to an organization's existence [82]. This information is often stored in an information asset inventory, as shown in Table 4 [82].

Table 4: Organization as Cloud Service Consumer Information Asset Inventory

Information Asset Category	Risk Management Component	Selected Asset List For Risk Management
People	Employees	Senior Manager
	Business Partners	Line Managers
	Students	Non-managerial employees

- **Information Asset Risk Sensitivity and Valuation**

Asset risk sensitivity is the crucial risk assessment component that dictates an organization's valuable assets, presented in table 4. As such, they are to be protected against any threat that could compromise the CIA-A's security objectives. [82] defines information asset risk sensitivity as a relative measurement of the tolerance of the resources for risk exposures. Determining the risk sensitivity scale will be based on several factors that are vital to an organization existence, factors such as :

- The most critical asset that contributes to the success of the organization
- The data classification scheme for information asset
- An investment that generates the most valuable profits and revenue
- An asset that is most expensive to protect and recover when compromised.
- Degree-of negative impact implications to an organization include Financial Loss, Legal Implications, Reputational Damages, and Regulatory Implications.

The Degree-of negative impact inflicted on an organization can result from compromised assets due to employees with poorly rated user behavior trust levels and associated risk rating. Both of these values will be a critical factor when determining an asset's risk sensitivity scale ratings. Integrating these key factors could help give an insight into risk and associated consequences, with an appropriate implementation of the *Trust-Based Adaptive Security Framework based on User Behavior* as a possible recommended mitigation solution.

Tables 5 and 6 [82] show that the Qualitative Risk sensitivity scale defines "People-Employees" asset sensitivity with detailed criteria to differentiate each sensitivity level.

Table 5: Qualitative Risk Sensitivity Scale

Level	Criteria
Low	A compromise would be limited and generally acceptable for the organization, resulting in minimal monetary, productivity, or reputational losses. There would be only minimal impact on normal operations or business activity
Medium	A compromise would be marginally acceptable for the organization, resulting in certain monetary, productivity, or reputational losses. Regular operations and/or business activity would be noticeably impaired, including the potential for breaches of contractual obligations
High	A compromise would be unacceptable for the organization, resulting in significant monetary, productivity, or reputational losses The ability to continue normal operations and/or business activity would be greatly impaired, potentially resulting in noncompliance with legal or regulatory requirements and/or loss of public confidence in the organization

With the qualitative scaling in place, Sensitivity Ratings are assigned to employees based on "User Behavior Trust Degree and User Behavior Risk Rating," as presented in Table 6 [82]. Thus, data classification will not affect the scale value. Still, it should be considered if the assessment is tailored to a specific Corporate Sector, private or public.

Table 6: Sensitivity Ratings for "People-Employees" Asset

Employee-ID	User Behavior Trust Degree	User Behavior Risk Rating	Sensitivity Rating	Data Classification Scheme
user-id-1	Complete Trust	Low	Low	Depends on Sector, either public or private sector
user-id_2	Partial Trust	Medium	Medium	Depends on Sector, either public or private sector
User-id_3	Not Credible	High	High	Depends on Sector, either public or private sector

- **Prioritization of Information Asset**

From Table 6, employees rated with the following profile; “High Sensitivity level, Not Credible and High-risk ratings” are considered a high priority for risk treatment due to the increased possibility to incurred critical risk. In this case, an employee identified as (User-id_3) is to be

treated first with the corresponding controls, followed by employees with lower profile values; in the next step of the Risk Management processes.

- **The Risk Management Approach**

The risk management approach will be based on the standard procedure of the ISO/IEC 27005:2018 Qualitative Risk Assessment approach guideline presented in figure 1.

- **Establish Risk Appetite, Threshold and Tolerance Declaration Statements**

These declarations could help organizations manage risk in the phase of continuous emerging threats.

Risk Appetite statement, a more generic risk appetite statement, will be appropriate for this process since it relates to all organizations that subscribe to SaaS regardless of the sector they belong to. The key objective is to maintain risks as low as possible that might be detrimental to the organization's existence. Risk impact or consequences might be deemed unacceptable and classified accordingly to Low-Risk Appetite, Moderate Risk Appetite, or High-Risk Appetite levels, depending on each organization's business goals and security objectives CIA-A. Treatment of each risk consequence with corresponding risk appetite level should be eminent within reasonable time and resources of the organization's capabilities.

Risk Threshold Statement, a senior management statement, expresses the amount of risk an organization is willing to accept regarding its business goals.

Risk Tolerance Statement, when risk appetite strategy could not be adhered to due to financial and resource constraints, senior management must deviate from the established low-risk appetite based on strategic and tactical plans. Risk exposure with adverse implications can shift from one with a lower risk appetite to one with a higher risk appetite. However, they must fall within the acceptable range from Negligible to High-risk rating. The risk with low appetite ratings is allowed deviation to risk with moderate risk appetite on the risk tolerance scale. The risk with moderate appetite ratings is allowed deviation to risk with higher moderate appetite on the Risk Tolerance scale.

The organization's Risk Appetite and Tolerance Declaration is based on due diligence and due care for senior managers to comply with organization governance controls. Top management should lower the sensitivity of some of its information assets and expectations to maintain the security objectives to one level down the previous one. This will ensure a more realistic risk exposure that will reasonably lie within the risk threshold. Of course, the elimination of risk is

practically impossible; as such, the main goal of any organization is to reduce risk in a cost-effective way that will fall within the acceptable risk threshold.

- **Risk Evaluation criteria**

Risk appetite, risk tolerance, and risk threshold should be used to compare each risk exposure and residual risk to determine its acceptability or not and conduct further assessment and apply risk treatment using the derived framework *Trust-Based Adaptive Security Framework based on User Behavior*.

- **Risk Estimation**

Based on the Qualitative Risk Assessment approach using the following variables:

  - Sensitivity of the People-Employees Asset - Qualitative Risk Sensitivity Scale (Derived from User Behavior Trust Degree and User Behavior Risk Rating)
  - Severity or Impact of the Vulnerability - Qualitative Severity/Impact Scale
  - Likelihood of the Threat - Qualitative Likelihood Scale

- **Impact Criteria**

Are based on the degree of damages inflicted on an organization's valuable asset with significant consequences such as Financial Losses, Reputational Damages, Regulatory Implications, and Legal Implications. As a result of employees who are negatively or poorly rated with “User Behavior Trust Degree and associated User Behavior Risk Rating values.”

- **Risk Acceptance Criteria**

This criterion will be associated with risk evaluation criteria, risk appetite, tolerance, and threshold.

5.2.2 Risk Analysis and Risk Treatment

- **Risk Analysis (Risk Identification)**

Risk identification is the process of identifying the following elements to estimate risk exposure. The components consist of:

1. Asset Identification: (People -Employees)

   People-Employees (Senior Manager, Line Managers, and Non-managerial employees) as detailed in Table 4. Employees are the most valuable asset to an organization and the weakest point in the information security chain. Senior managers are responsible for executing critical business decisions at the strategic level and enforcing governance controls through due diligence and due care. Line managers at the next lower level of any organization chat are responsible for executing tactical business decisions based on the business decision made at the strategic level by senior managers. In contrast, non-managerial employees take day-to-day business operations from the strategic to an operational level. Regardless of the employee's position and commitment, the level of risk impact on a business process or other valuable asset when compromised will still be the same because the end goal is to cause financial loss, reputational damages, regulatory and legal implications. Therefore, for the sake of the risk assessment, employees will be considered single an asset regardless of their position and responsibilities based on the fact that risk impact as a result of compromise will make little or no difference with regards to the degree of damages inflicted on the organization. Employees' assets are tagged as ***user-id-xxx.***

2. Identified Vulnerabilities

Common vulnerabilities found within the SaaS environment with regards to cloud users are known to consist of: -

- Weak Identity, Credential, and access management

  Some Cloud users tend to use weak passwords, credential abuse, stolen by attackers to impersonate legitimate cloud users, and careless password management [94]. This can lead to the disclosure of sensitive information, unauthorized manipulation, or destruction of the system; worst case, the affected account is an account with privileged access.

- Absence or ineffective access control mechanism

  The absence or existence of ineffective access control mechanisms can lead to unauthorized access and compromised cloud resources. Possible compromise can be loss of confidentiality, integrity, and asset availability. Furthermore, lack or ineffective access control can facilitate unauthorized access to install malware programs on a critical system to perform malicious activities that fulfill the attacker's goal. It can also give malicious insiders such as disgruntle employees to conduct malicious acts against the organization.

- Lack of Security Awareness against Social Engineering.

  This leads to non or limited knowledge of security threats and risks that pose a severe threat to the organization. Employees can be subjected to social engineering attacks like phishing attacks and scams.

- Careless or Incompetent System Administrator
  Can facilitate a disgruntled employee or malicious insider conduct sabotage, espionage to steal sensitive information for business benefits. Even cause system failures, data corruption, information disclosure because of mistake, or improper password management.

- Improper handling of sensitive or confidential information by employees.
  Due to lack of security mechanism in place or sufficient knowledge of how the procedure works or incompetency of the employee can lead to security breaches or loss of data classified as sensitive or confidential.

3. Identified Threats

Referring to section 2.5.3 SaaS Security Issue detailed in *The Treacherous Twelve' Cloud Computing Top Threats in 2016* [5], are common threats that are known to exploit the listed vulnerabilities in the previous section consist of:

- Incompetent System Administrator
  A careless or incompetent system administrator with little or no knowledge of the risk it can impose on the organization is a significant threat if an administrative account with privileged access is involved or lacks technical expertise. The most common impact can be loss of service availability, loss, or leakage of sensitive information.

- Malicious Insider
  A disgruntled employee or malicious insider can sabotage, espionage, and steal sensitive information for illegal business benefits contrary to the organization's business interest.

- Data Breaches and Data Loss
  Unauthorized access of sensitive information either through sabotage, stolen or data loss, or Sensitive information leakage. Possible exploit on absence or ineffective access control mechanism, and weak Identity, credential, access management.

- Account Hijacking and Account Misuse
  Stolen accounts for impersonation of a legitimate employee to have unauthorized access to cloud resources, then to further conduct activities. Account misuses due to misuse of privileged right and permission because of weak Identity, credential, access management, and absence or ineffective access control mechanism

- Man-In-The-Middle
  An act of malicious intruder impersonates and positions themselves between communication paths to gain unauthorized access to confidential information, conduct unauthorized data manipulation, or even provoke service unavailability when a legitimate employee's account is compromised. The attack is possible due to a combination of weak identity, credential, and access management vulnerabilities and the absence of a weak encryption algorithm for data being transmitted capture through packet sniffers.

  - Malware Infection

  One of the significant issues impacting any organization is employees who fall victims to phishing attacks, accessing malicious websites, and installing software infected with malware code can be used as a threat vector to exploit and compromise the organization's cloud resources. Compromised systems can be subjected to various types of attacks, for example, destruction of system components through Virus, the technique used as Botnet for C2C network by Trojan Horse, propagation of other forms of malware in the case of Worms, modify system codes to suites attackers purpose, encrypting of compromised systems components to request a ransom before releasing the decryption keys back to the victims by the use of crypto-malware such as ransomware.

- Social Engineering (Phishing, Whaling, Spear phishing, Scam)

The act of tricking someone into gaining valuable information from that person Phishing legitimately can be done via scam emails with malicious attachments or embedded links to malicious websites. Phishing attacks easily exploit employees with no security awareness training by clicking the suspicious links to malicious websites and probably their accounts being hijacked or sniffed to enable further malicious activities—downloading malicious contents with embedded malware. The consequences of such acts lead to security compromise of the organization through the employee's actions.

- Drive-By Download (Malware Distributor)

A threat where an attacker conducts a stealth download and installation of a malicious payload to employees' systems without their knowledge when they visit suspicious websites that host malicious contents. In most cases is to prepare the environment for a future attack.

- Loss of Service Availability

  Loss of availability is highly possible due to careless or incompetent system administrators with as authorized users with privileged account permissions with little or no knowledge of the expertise required to conduct the task or lack of risk awareness.

- **Risk Analysis (Risk Estimation)**

Based on the Qualitative Risk Assessment approach using the following variables:

- Sensitivity of the People-Employees Asset - Qualitative Risk Sensitivity Scale (Derived from User Behavior Trust Degree and User Behavior Risk Rating)
- Severity or Impact of the Vulnerability - Qualitative Severity/Impact Scale
- Likelihood of the Threat - Qualitative Likelihood Scale

1. <u>Sensitivity of the People-Employees Asset - Qualitative Risk Sensitivity</u>

An employee with ***user-id_3***, from table 6 [82], is chosen as a sample for the risk assessment. The reason is due to the following employee profile attributes; Not Credible -User Behavior Trust Level, High -User Behavior Risk Rating, and High -Sensitivity Rating [82].

2. Impact of the Vulnerability - Qualitative Severity-Impact Scale

Threat: Account Hijacking and Account Misuse

Vulnerability: Weak Identity, Credential, and Access Management

Asset	Impact on Financial Loss/Revenue (1/10)	Impact on Legal Implication (1/10)	Impact on Reputation (1/10)	Impact on Regulation (1/10)	Impact (/40)
Employee (*user-id-3*)	**8**	**5**	**8**	**5**	**26**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	Description
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	**Extreme**	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	**Critical**
High	Moderate	High	Critical
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Man-In-The-Middle

Vulnerability: Weak Identity, Credential, and access management

Asset	**Impact on Financial Loss/Revenue** (1/10)	**Impact on Legal Implication** (1/10)	**Impact on Reputation** (1/10)	**Impact on Regulation** (1/10)	**Impact** (/40)
Employee ***(user-id-3)***	**8**	**4**	**8**	**4**	**24**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	**Description**
Certain	Expected to occur in most circumstances, more than once a year

Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	**High**	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

- **Extreme** = action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	Critical
High	Moderate	High	**Critical**
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical** = action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Malware Infection

Vulnerability: Absence or ineffective access control mechanism

Asset	Impact on Financial Loss/Revenue (1/10)	Impact on Legal Implication (1/10)	Impact on Reputation (1/10)	Impact on Regulation (1/10)	Impact (/40)
Employee (*user-id-3*)	**8**	**6**	**8**	**6**	**28**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	Description
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	**Extreme**	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

- **Extreme**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	**Critical**
High	Moderate	High	Critical
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Malicious Insider

Vulnerability: Absence or ineffective access control mechanism

Asset	Impact on Financial Loss/Revenue (1/10)	Impact on Legal Implication (1/10)	Impact on Reputation (1/10)	Impact on Regulation (1/10)	Impact (/40)
Employee (*user-id-3*)	**8**	**6**	**5**	**3**	**22**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	Description
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	**High**	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

- **Extreme**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	Critical
High	Moderate	High	**Critical**
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical** = action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Social Engineering (Phishing, Whaling, Spear phishing, Scam)

Vulnerability: Lack of Security Awareness

Asset	**Impact on Financial Loss/Revenue (1/10)**	**Impact on Legal Implication (1/10)**	**Impact on Reputation (1/10)**	**Impact on Regulation (1/10)**	**Impact (/40)**
Employee (*user-id-3*)	**8**	**6**	**8**	**7**	**29**

Insignificant < 15, and means we can deal with as a part of routine operations

- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	**Description**
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	**Extreme**	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

- **Extreme**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	**Critical**
High	Moderate	High	Critical
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Malware Infection

Vulnerability: Lack of Security Awareness

Asset	Impact on Financial Loss/Revenue (1/10)		Impact on Legal Implication (1/10)	Impact on Reputation (1/10)	Impact on Regulation (1/10)	Impact (/40)
Employee (*user-id-3*)	**8**		**6**	**8**	**7**	**29**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	Description
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	**Extreme**	Extreme
Possible	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	**Critical**
High	Moderate	High	Critical
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Drive-By Download (Malware Distributor)

Vulnerability: Lack of Security Awareness

Asset	**Impact on Financial Loss/Revenue (1/10)**	**Impact on Legal Implication (1/10)**	**Impact on Reputation (1/10)**	**Impact on Regulation (1/10)**	**Impact (/40)**
Employee (*user-id-3*)	**7**	**5**	**7**	**5**	**24**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	**Description**
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	**High**	Extreme	Extreme
Possible	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme

- **Extreme**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	Critical
High	Moderate	High	**Critical**
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Loss of Service Availability
Vulnerability: Careless or Incompetent System Administrator

Asset	**Impact on Financial Loss/Revenue (1/10)**	**Impact on Legal Implication (1/10)**	**Impact on Reputation (1/10)**	**Impact on Regulation (1/10)**	**Impact (/40)**
Employee (*user-id-3*)	**8**	**3**	**8**	**3**	**22**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	**Description**
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	**High**	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	Critical
High	Moderate	High	**Critical**
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Extreme**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Data Breaches and Data Loss

Vulnerability: Careless or Incompetent System Administrator

Asset	Impact on Financial Loss/Revenue (1/10)	Impact on Legal Implication (1/10)	Impact on Reputation (1/10)	Impact on Regulation (1/10)	Impact (/40)
Employee (*user-id-3*)	**8**	**7**	**8**	**8**	**31**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	Description
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	Extreme	**Extreme**
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	**Critical**
High	Moderate	High	Critical
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Critical**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Threat: Data Breaches and Data Loss

Vulnerability: Improper handling of sensitive

Asset	**Impact on Financial Loss/Revenue (1/10)**	**Impact on Legal Implication (1/10)**	**Impact on Reputation (1/10)**	**Impact on Regulation (1/10)**	**Impact (/40)**
Employee (*user-id-3*)	**8**	**7**	**8**	**8**	**31**

- Insignificant < 15, and means we can deal with as a part of routine operations
- Low >= 15, < 20, and can affect the effectiveness of business, and indirect costs
- Medium >= 20, < 25, and means asset need to be reviewed not to incur costs
- High >= 25, < 30, and means that major problems will incur financial costs
- Catastrophic >= 30, will lead to direct and significant financial loss

Likelihood of the Threat - Qualitative Likelihood Scale

Level	**Description**
Certain	Expected to occur in most circumstances, more than once a year
Likely	will probably occur in most circumstances, once every year
Possible	Might occur at some time, once every 5 years
Unlikely	Could occur at some time, once every 10 years
Rare	May occur or only in exceptional circumstances, once every 20 year

Risk Rating Matrix (without with Qualitative Risk Sensitivity) **Impact- Severity**					
Likelihood	**Insignificant**	**Low**	**Medium**	**High**	**Catastrophic**
Almost certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	Extreme	**Extreme**
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) **Risk Sensitivity**			
Risk Rating Matrix (Likelihood + Impact)	**Low**	**Moderate**	**High**
Extreme	High	Critical	**Critical**
High	Moderate	High	Critical
Moderate	Low	High	Critical
Low	Low	Moderate	High

- **Extreme**= action required immediatly
- **High** = attention by senior management required
- **Moderate** = specify management responsibility
- **Low** = routine procedure required

[83]

Table 7: Qualitative Risk Assessment - Risk Registry

Risk Register with No Controls								
Asset	Vulnerability	Impact (severity)	Threat	Likelihood	Risk Level without Risk Sensitivity	Risk Sensitivity	Risk Level with Risk Sensitivity Scale	Controls (Adaptive Security Control Engine)
Employee (user-id-3)	Weak Identity, Credential, and access management	High	Account Hijacking and Account Misuse	Certain	Extreme	High	Critical	Preventive Control Process (Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy), Security Policies and Procedure ,Security Awareness Program) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system Retrospective Control Process (Conduct Incident Response) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk, Baselining security posture)
Employee (user-id-3)	Weak Identity, Credential and access management	Medium	Man-In-The-Middle	Possible	High	High	Critical	Preventive Control Process (Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy) ,Security Awareness Program, Implement Encryption Mechanism, Enforce End-Point Security Data Prevention Leakage, Hardening and Isolation, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk, Baselining security posture)
Employee (user-id-3)	Absence or ineffective access control mechanism	High	Malware Infection	Possible	Extreme	High	Critical	Preventive Control Process (Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy), Security Policies and Procedure ,Security Awareness Program, Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies

								identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk, Baselining security posture)
Employee (user-id-3)	Absence or ineffective access control mechanism	Medium	Malicious Insider	Possible	High	High	Critical	Preventive Control Process Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy, Security Policies and Procedure ,System Hardening and Isolation, Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Lack of Security Awareness	High	Social Engineering (Phishing, Whaling, Spear phishing, Scam)	Certain	Extreme	High	Critical	Preventive Control Process (Security Awareness Program, Security Policies and Procedure, Enforce Access control Procedures (user accounts),Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Lack of Security Awareness	High	Malware Infection	Likely	Extreme	High	Critical	Preventive Control Process (Security Awareness Program, Security Policies and Procedure,Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage,Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct

								to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Lack of Security Awareness	Medium	Drive-By Download (Malware Distributor)	Likely	High	High	Critical	Preventive Control Process Security Awareness Program, Security Policies and Procedure, Enforce End-Point Security-Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Careless or Incompetent System Administrator	Medium	Loss of Service Availability	Possible	High	High	Critical	Preventive Control Process (System Hardening and Isolation, Security Policies and Procedure) Detective Control Process (Logging, real-time monitoring and alerts , system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Careless or Incompetent System Administrator	Catastrophic	Data Breaches and Data Loss	Possible	Extreme	High	Critical	Preventive Control Process (System Hardening and Isolation, Security Policies and Procedure, Enforce End-Point Security Data Prevention Leakage) Detective Control Process (Logging, real-time monitoring and alerts , system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Improper handling of sensitive	Catastrophic	Data breaches and Data Loss	Possible	Extreme	High	Critical	Preventive Control Process (Security Policies and Procedure, Enforce End-Point Security Data Prevention Leakage) Detective Control Process (Logging, real-time monitoring and alerts , system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)

Risk Treatment

After implementing the framework for each risk treatment, it is noticeable that the user sensitivity risk ratings were reduced from high to low. The primary reason for this reduction was a change in the user behavior, which eventually increased the trust level and decreased the risk level—ultimately influencing the sensitivity risk ratings, seamlessly reducing each identified risk, as presented in Table 8: Risk Register and Risk Monitor.

Table8: Risk Register After Implemented (Adaptive Security Controls) and Degraded Risk Sensitivity - (Risk Monitor)

Asset	Vulnerability	Threat	Impact (severity)	Likelihood	Risk Level without Risk Sensitivity	New Risk Sensitivity	Risk Level with Risk Sensitivity Scale
Employee (user-id-3)	Weak Identity, Credential and access management	Account Hijacking and Account Misuse	Medium	Likely	High	Low	Moderate
Employee (user-id-3)	Weak Identity, Credential and access management	Man-In-The-Middle	Insignificant	Rare	Low	Low	Low
Employee (user-id-3)	Absence or ineffective access control mechanism	Malware Infection	Medium	Unlikely	Moderate	Low	Low
Employee (user-id-3)	Absence or ineffective access control mechanism	Malicious Insider	Low	Unlikely	Low	Low	Low
Employee (user-id-3)	Lack of Security Awareness	Social Engineering (Phishing, Whaling, Spear phishing, Scam)	Medium	Possible	High	Low	Moderate
Employee (user-id-3)	Lack of Security Awareness	Malware Infection	Medium	Possible	High	Low	Moderate
Employee (user-id-3)	Lack of Security Awareness	Drive-By Download (Malware Distributor)	Low	Possible	Moderate	Low	Low
Employee (user-id-3)	Careless or Incompetent System Administrator	Loss of Service Availability	Low	Possible	Moderate	Low	Low
Employee (user-id-3)	Careless or Incompetent System Administrator	Data breaches and Data Loss	High	Unlikely	High	Low	Moderate
Employee (user-id-3)	Improper handling of sensitive	Data breaches and Data Loss	High	Unlikely	High	Low	Moderate

Chapter 6
Results

The presentation of the results will be divided into two sections as shown below, with a final evaluation if the design and implementation have met our goal of resolving the research problem:

- Phase 1: Design: *Trust-Based Adaptive Security Framework based on User Behavior*.
- Phase 2: Implementation: *Trust-Based Adaptive Security Framework based on User Behavior.* As Risk Mitigation Solution in Risk Management process ISO/2705:2018

6.1 Phase 1 Design: Trust-Based Adaptive Security Framework based on User Behavior.

The design phase figures 18, 19, and 20 from sections *Low-Level System Design presentation and Operational Functionality* are reproduced here to help explain the illustrated work and the resulting outcome. Enforcement of the dynamic access control started with an authenticated user initially granted or denied permission by the adaptive security system through consultation of the RBAC authorization server concerning the user permission attributes. Next, other system components conduct further authorization assessments as more granular access control measures to manage the initial access granted effectively. The outcome of the entire process can be considered a hierarchy of access control measures based on the user identity and how the user behaves across the cloud after being granted initial access.

The subsequent sections outline each system component's functionality and the resulting outcome. It is essential to notice that each system has interconnected channels connecting it to other data, signals, and information exchanges or transmission. Input and output data are vital for the proper functioning of the solution as a whole system.

6.1.1 User Behavior Trust Manager

The user behavior trust manager presented in figure 20 is one of the crucial components of the framework that evaluates the user's activities and computes the actual trust level of each user. After users are granted access to the SaaS infrastructure through the RBAC authorization process, their activities are forwarded to and collected by behavior trust evidence collection. As presented in Figure 20, *User Behavior Trust Evaluation Process*, User activities reflect individual behavior concerning access permission and the usage of SaaS resources. Each user behavior trust evidence is collected as logs information from different log sources across the SaaS infrastructure.

Examples of this log information are; User Login Information, Security Evidence, Operation Habits, Performance Metrics, Reliability Characteristics, and Abnormal operation. They are later parsed into a standard log format, correlated, and then analyzed by the Behavior Data Analysis process. Finally, the output is fed into the Trust Evaluation, and the computation process computes the Direct Trust Degree of the user.

Additionally, recommendations from different cloud service providers and entities within the same cloud service domain with direct interaction are also collected and synthesized, then fed into the Trust Evaluation and computation process to compute each user recommendation, eventually forming the Recommendation Trust Degree. Each user has recorded historical data to calculate the user's Historical Trust Degree. The historical trust degree is regularly updated based on ongoing activities with associated behavior during user access. To determine the overall user behavior trust level or degree, a weighted value is applied across previously computed trust types of; Direct Trust Degree, Recommendations Trust Degree, and Historical Trust Degree to determine the Comprehensive Trust Degree. The evaluation and computation of each user's trust level is an ongoing assessment that tends to reflect the user's current trust level regardless of the access granted previously. Based on the variation of each user's behavior regarding access activities, the user's trust level can either be degraded by punishment or increased. Afterward, used to update the user behavior trust list and recent historical trust degree. The updated trust list is essential for keeping the historical trust accurate and up to date for continuous computation of the user's new comprehensive trust degree. Copies of the updated trust list are stored in the trust degree and risk rating database, in addition to user behavior risk ratings, for future use by other processes, most importantly, the policy decision point central server.

The computed user behavior risk rating and comprehensive user behavior trust degree by the *User Behavior Trust Manager* form the primary link and parameters for the outbound risk assessment process of ISO/IEC 27005:2018 *Sensitivity Ratings People-Employees Asset* presented previously in Table 6.

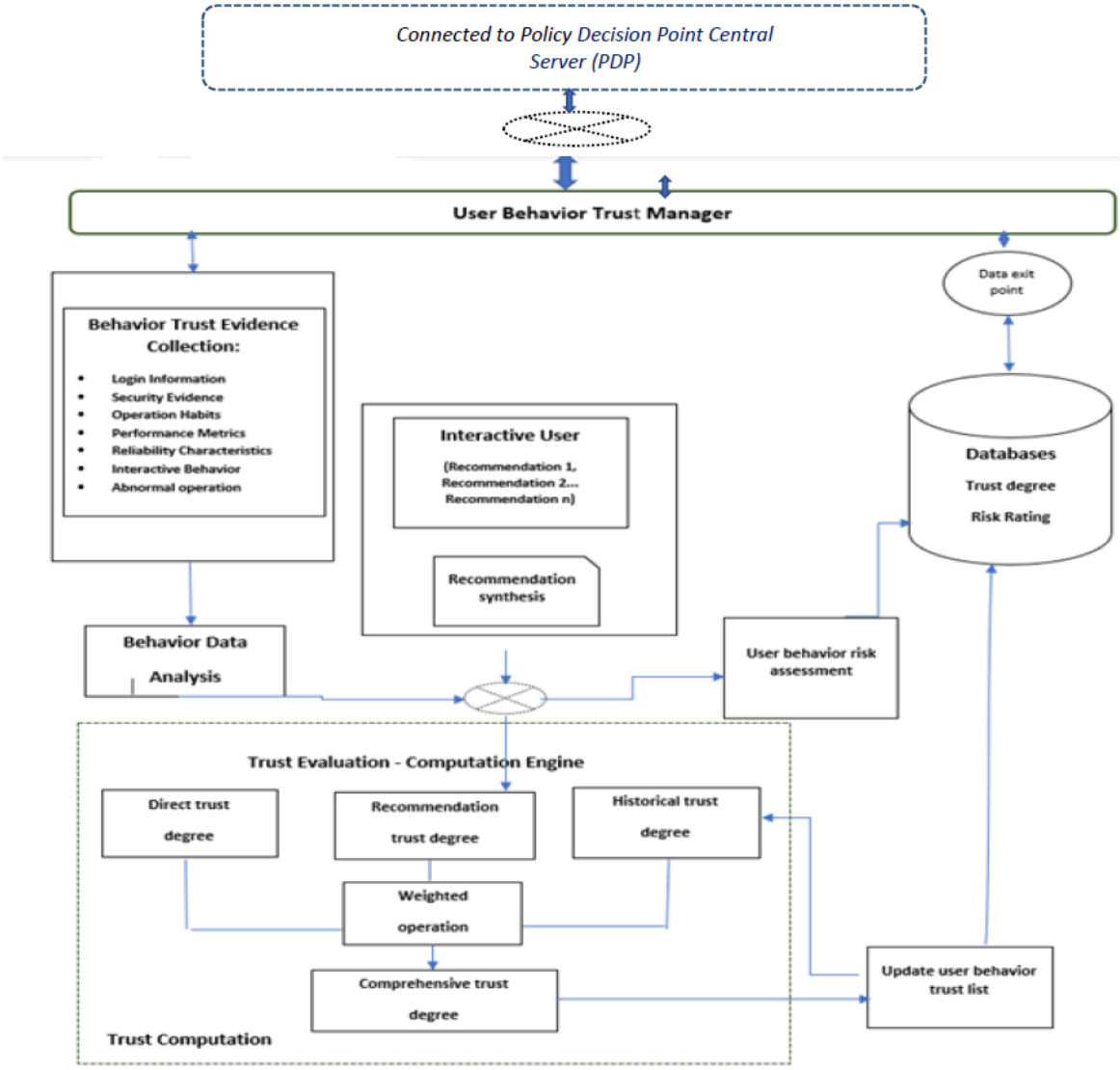


Figure 20: Process of Trust Evaluation

6.1.2 Policy Decision Point (PDP) Central Server

The policy decision point server processes the inputs it retrieved from the trust manager's database to make an authorization and access control decision that the corresponding adaptive security engine will enforce. To effectively process access control decisions, each user trust and risk levels' current state was categorized into "Complete Trust, Partial Trust, and Not Credible" and risk rating of "High, Medium, and Low Risk."

The Logical processor performs the process of determining and assigning what trust level corresponds to each user, as presented in figure 19-b. It conducts the low-level processing by evaluating the "Comprehensive Trust Degree" against the "Abnormal Threshold" set; a fixed value, plus each user behavior "Risk Rating" value. User with a comprehensive trust lower than

the abnormal threshold plus risk rating equals low will be assigned a “Complete Trust” and marked for “Grant full access.”. While users with comprehensive trust less than the abnormal threshold but with a medium risk rating will be assigned “Partial Trust” and then marked as “Grant limited access.” Lastly, a user with comprehensive trust greater than an abnormal threshold and high-risk rating will be assigned “Not Credible Trust,” will be marked as “Deny access.”

The low-level process performs the logical operation as in figure 19-b, which is then interpreted by the high-level function in figure 19-a using the parameters derived from the low-level process operation to make the decision process visible to the adaptive security engines by sending the outcome through signaling or data communication. Users with complete trust and low-risk ratings are tagged with granted full access, while a user with partial trust is labeled with granted limited access, and lastly, a user with not credible trust is labeled with granted no access.

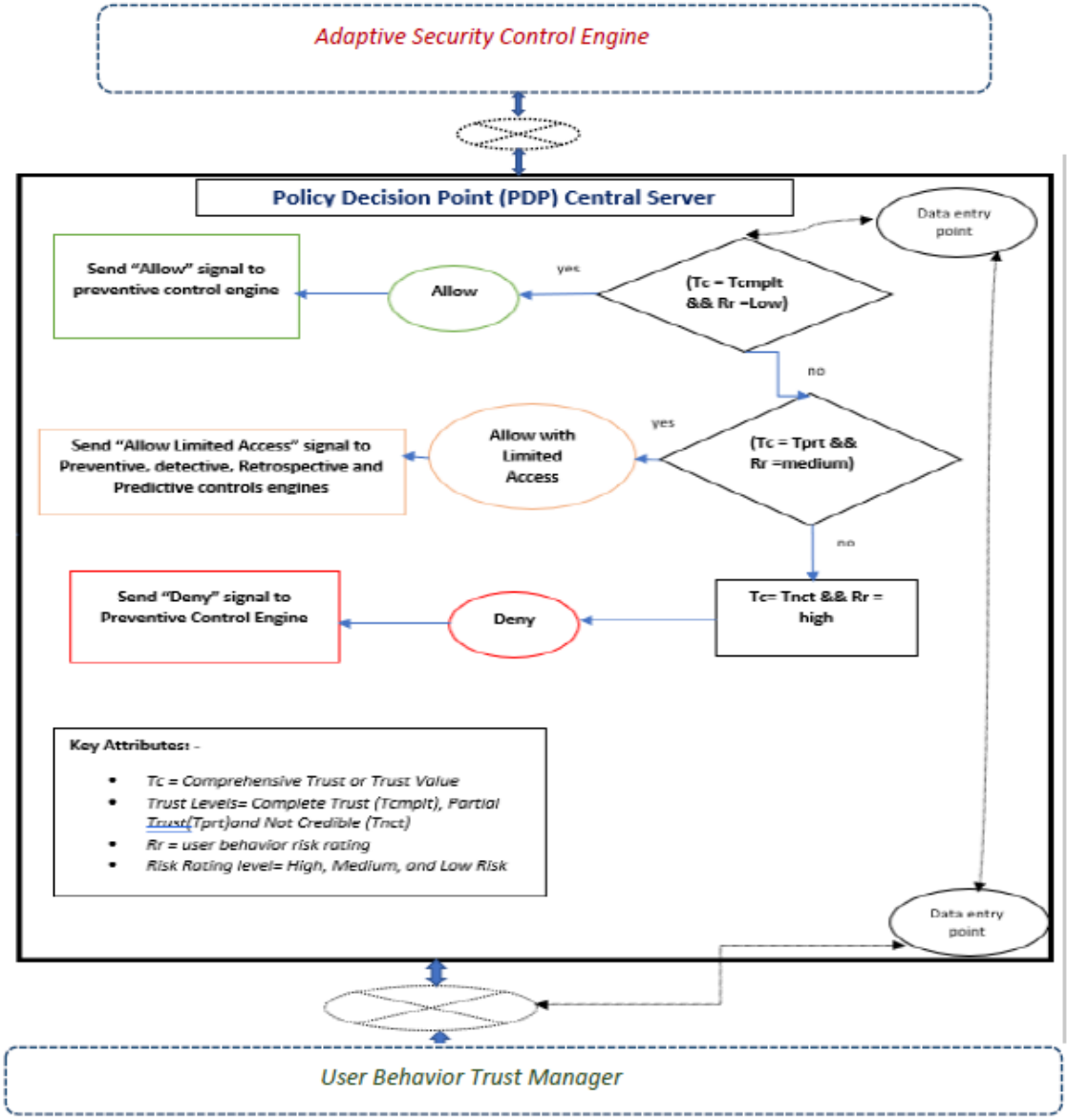
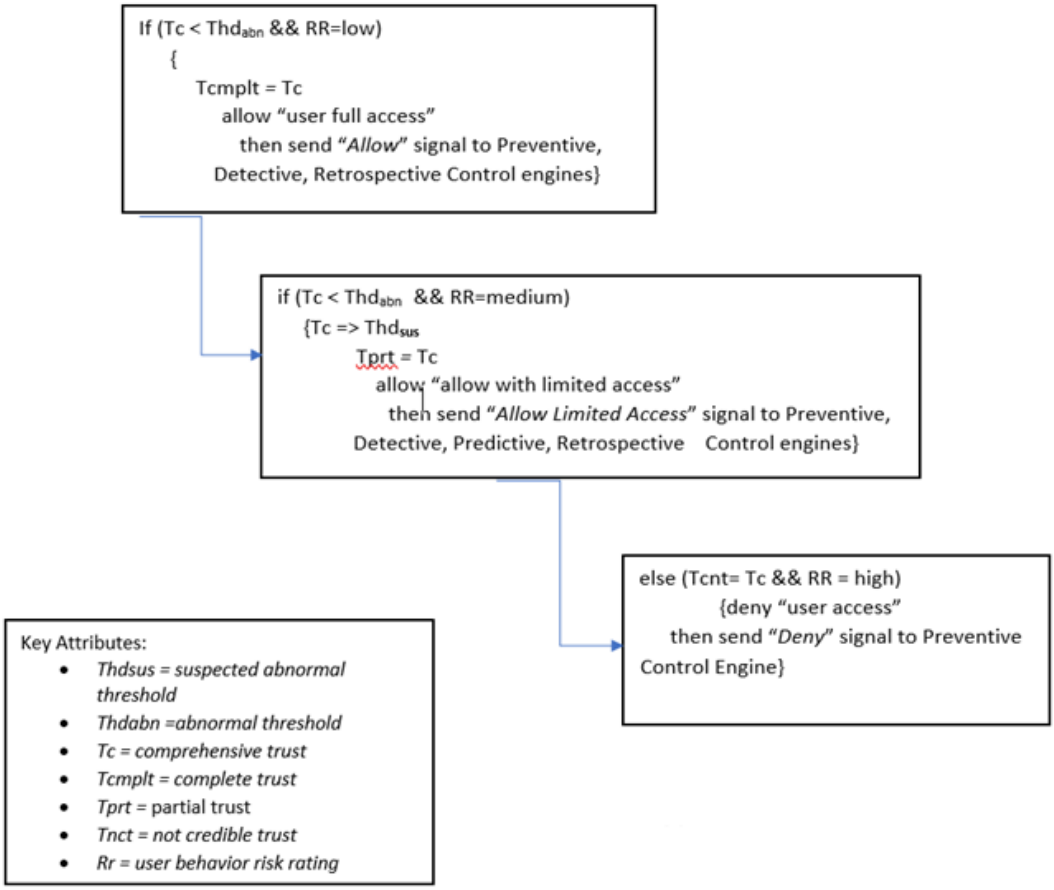


Figure 19-a. Decision-making process - user behavior trust and risk access control



Each outcome is sent to the corresponding adaptive security processor to enforce the corresponding control partnering to each user behavior from their activities.

Figure 19-b. Decision-making process- Logical Processor

6.1.3 Adaptive Security Control Engine

The adaptive security control engines function as control enforcement points. It consists of four types of controls; preventive, detective, retrospective or respond, and predictive controls capabilities. Depending on the kind of decision signal received from the policy decision point server, about user behavior trust level and associated risk rating, in conjunction with other environmental or context factors, it enforces one or multiple types of controls to mitigate the actual threat and risk identified. Figure 18 presents the types of controls imposed on users based on their trust and risk level when accessing and utilizing SaaS resources. The controls are applicable or integrated into the continuous risk management process to enhance cloud users' identity and access control.

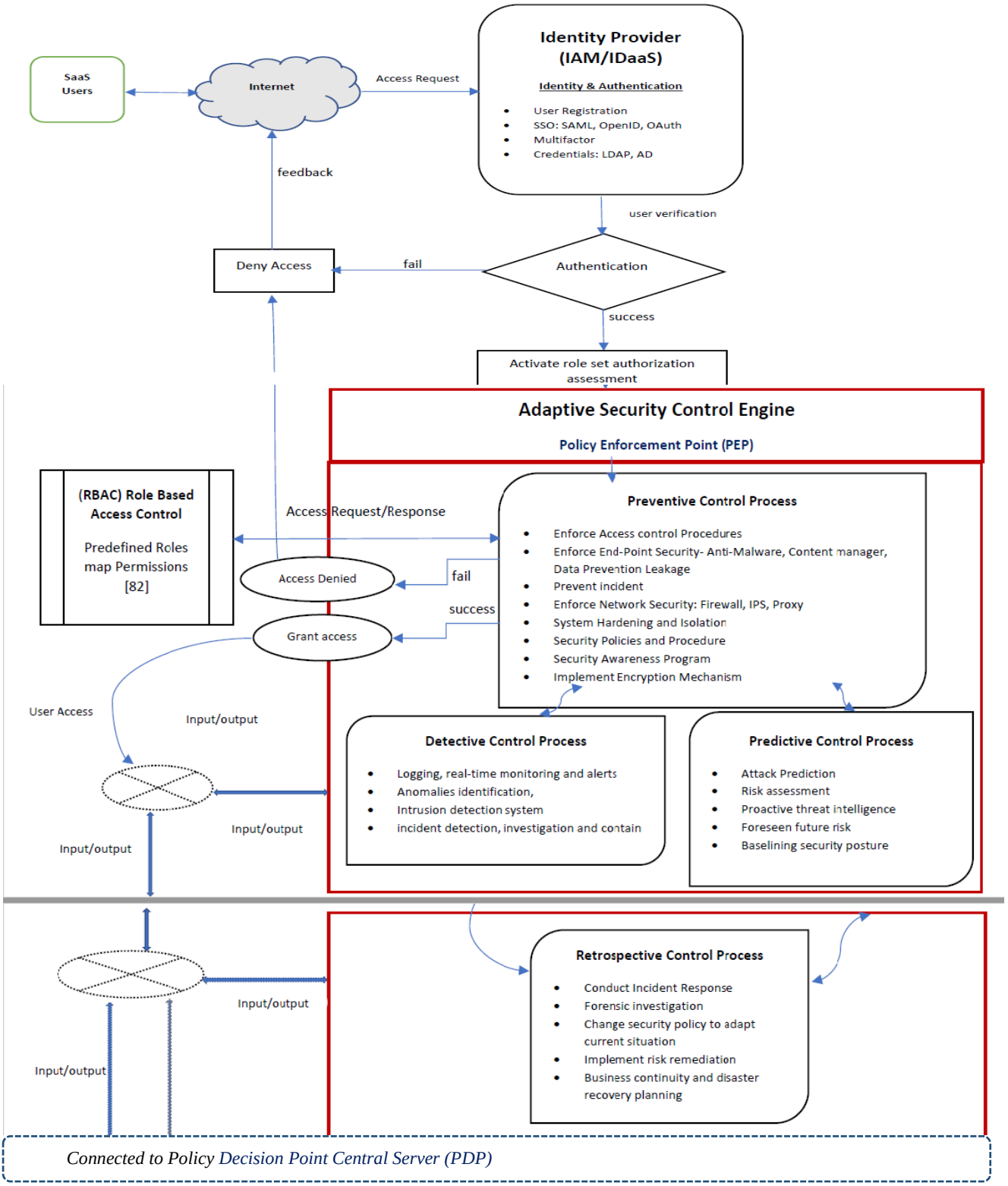


Figure 18: Process of Adaptive Security Architecture [78]

6.2 Phase 2 Implementation: Trust-Based Security Framework based on User Behavior. "As Risk Mitigation Solution in Risk Management process ISO/2705:2018."

This section outlines the risk assessment process and how the designed framework solution is integrated and used as a possible risk mitigation solution to resolve various identified risks relating to user identity and access management issues when accessing and utilizing the SaaS resource. The process starts by defining a context for the risk management process, which elaborates on people assets. People asset valuation is based on risk sensitivity as a critical factor used to determine an asset value. User behavior trust degree and associated risk rating directly influence the risk sensitivity factor. Next, risk analysis was conducted to identify people entities (SaaS users) as valuable assets, threats, and vulnerabilities associated with the asset. Next, risk identification through the risk estimation process in conjunction with risk evaluation to prioritize which risk should be treated first. Lastly, applying the risk mitigation solution *Trust-Based Adaptive Security Framework based on User Behavior.* as a possible risk treatment solution for each identified risk, threat, and vulnerability to people(user) entity asset.

6.2.1 Context Establishment

Information assets and scope are specified within context establishment, and the primary purpose is to identify and categorize information assets. It can be defined as the process of collecting data, data set, or any asset that collects, processes, transmit, or store information valuable to an organization's existence. This information is often stored in an information asset inventory, as shown in Table 4 [82].

Table 4: Organization as Cloud Service Consumer Information Asset Inventory

Information Asset Category	Risk Management Component	Selected Asset List For Risk Management
People	Employees	Senior Manager Line Managers Non-managerial employees
	Business Partners	
	Students	

Risk sensitivity and its influences on asset valuation were performed to help determine how critical and valuable the identified information asset (people) in table 4 are relevant to the existence of any organization, in addition to why the people asset and cloud service should be protected against a threat that might compromise CIA-A's security objectives. Information asset risk sensitivity is "A relative measurement of the tolerance of the resources for risk exposures, similar to an evaluation of

criticality or importance to the organization, independent of any particular threat or vulnerability" [82]. Therefore, asset risk sensitivity was the key factor used to determine asset valuation.

The degree-of negative impact inflicted on an organization results from poorly rated employee's behavior trust degree and behavior risk rating; computed by the user behavior trust manager. Both parameters, behavior trust degree and behavior risk rating, are essential when formulating the risk sensitivity scale ratings—as such, integrating user behavior trust and associated risk rating could give insight into the degree-of negative impact. Therefore, implementing the *User Behavior Trust-Based Adaptive Security Framework* as a possible mitigation solution is recommended. In addition, Tables 5 and 6 [82] show that the Qualitative Risk sensitivity scale defines "People-Employees" asset sensitivity with detailed criteria to differentiate each sensitivity level.

Table 5: Qualitative Risk Sensitivity Scale

Level	Criteria
Low	A compromise would be limited and generally acceptable for the organization, resulting in minimal monetary, productivity, or reputational losses. There would be only minimal impact on normal operations or business activity
Medium	A compromise would be marginally acceptable for the organization, resulting in certain monetary, productivity, or reputational losses. Regular operations and/or business activity would be noticeably impaired, including the potential for breaches of contractual obligations
High	A compromise would be unacceptable for the organization, resulting in significant monetary, productivity, or reputational losses The ability to continue normal operations and/or business activity would be greatly impaired, potentially resulting in noncompliance with legal or regulatory requirements and/or loss of public confidence in the organization

With the qualitative scaling in place, Sensitivity Ratings are assigned to employees as presented in Table 6 [82], based on "User Behavior Trust Degree and User Behavior Risk Rating*";* these values were obtained from the Trust Evaluation & Computation user behavior risk assessment process. Data classification does not affect the scale value. Still, it should be considered if the assessment is tailored to a specific corporate sector, either the private or public sector. **User-id_3** was assigned a prioritized asset for risk treatment due to its high-risk value and non-credible trust level. Therefore, chosen as an asset sample for the next stage of the risk analysis process.

Table 6: Sensitivity Ratings for "People-Employees" Asset

Employee-ID	User Behavior Trust Degree	User Behavior Risk Rating	Risk Sensitivity Rating	Data Classification Scheme
user-id-1	Complete Trust	Low	Low	Depends on Sector, either public or private sector
user-id_2	Partial Trust	Medium	Medium	Depends on Sector, either public or private sector
User-id_3	Not Credible	High	High	Depends on Sector, either public or private sector

The chosen Risk Management methodology was the ISO/IEC 27005:2018 with a Qualitative Risk assessment approach detailed in figure 1. Statements or declarations for; risk appetite, tolerance, and threshold were also established and signed-off by senior management as part of governance compliance. The declared statements reflect what risks and deviations are acceptable to any organization using the SaaS cloud environment. Sample's statement of the organization's risk appetite and tolerance declarations should be based on due diligence and due care to comply with the organization's governance controls. Top management should lower some of its information assets' sensitivity and expectations to maintain its security objectives one level lower. Furthermore, it provides a better insight into organization risk exposure that might reasonably lie within the risk threshold. The elimination of risk is practically impossible; as such, the main goal of any organization is to reduce risk in a cost-effective manner that should fall within the acceptable risk threshold.

Risk Evaluation criteria were based on comparing the declared risk appetite, risk tolerance, and risk threshold to each identified risk exposure and residual risk to determine its acceptability, conduct further assessment and apply risk treatment using the derived framework *User Behavior Trust-Based Adaptive Security Framework*.

Risk Estimation was based on the Qualitative Risk Assessment approach using the following variables; Sensitivity of the People-Employees Asset - Qualitative Risk Sensitivity Scale derived from User Behavior Trust Degree and User Behavior Risk Rating, Severity or Impact of the Vulnerability - Qualitative Severity/Impact Scale, Likelihood of the Threat - Qualitative Likelihood Scale.

Impact criteria were based on the degree of damages inflicted on an organization's valuable asset with significant consequences such as Financial Losses, Reputational Damages, Regulatory Implications, and Legal Implications. As a result of users who are poorly rated with user behavior trust degree and behavior risk rating. At the same time, risk acceptance criteria were associated with risk evaluation criteria, risk appetite, tolerance, and threshold.

6.2.2 Risk Analysis

Asset identification focuses on People -Employees assets, as the framework was designed and tailored exclusively towards user entity as a subject requesting access to SaaS resources objects. People-Employees were classified based on their roles and responsibility within an organization, such as Senior Manager, Line Managers, and Non-managerial employees, as detailed in Table 4. Regardless of the employee's position and commitment, the level of risk impact on a business process or other valuable asset when compromised, will remain the same since the end goal is to cause financial loss, reputational damages, regulatory and legal implications.

Within the risk assessment process, employees are considered a single asset regardless of their position and responsibilities based on the fact that risk impact as a result of a compromise will make little or no difference when considering the degree of damages that could be inflicted on the organization. Therefore, employees assets presented in Table 6 were tagged as user-id-xxx, where user-id-3 was selected as a sample asset for the risk estimation process.

Common vulnerabilities found within the SaaS environment associated with cloud users include the following; Weak Identity, Credential, and access management (a vulnerability where cloud users use a weak password, credential abuse, improper protection of credentials that can facilitate an attacker stealing the credentials to impersonate legitimate cloud authorized user). The absence or existence of ineffective access control mechanisms can lead to unauthorized access and compromised cloud resources. Lack of threat security awareness leads to non or limited knowledge of security threats and risks that will pose a severe threat to the organization. Employees can be subjected to social engineering attacks like phishing attacks and scams. Careless or Incompetent system administrator can facilitate a disgruntled employee or malicious insider to conduct sabotage, espionage to steal sensitive information or cause system failures, data corruption, information disclosure because of mistake, or improper password management, Improper handling of sensitive or confidential information by the user due to lack of security mechanism in place or sufficient knowledge of how the procedure works or incompetency of the employee can lead to security breaches or loss of data classified as sensitive or confidential.

Common threats that could exploit the listed vulnerabilities tied to cloud users were also identified. The most common threats published by *The Treacherous Twelve' Cloud Computing Top Threats in 2016* [4] consist of*;* Incompetent System Administrator as result of with little or no knowledge of the risk it can impose on the organization is a significant threat, for example, day to day usage of administrative account with privilege access is carelessly handled or lack of technical expertise to the job at hand. The most common impact can be loss of service availability, loss, or leakage of sensitive information. User as a Malicious Insider, for example, a disgruntled employee who can sabotage espionage to steal sensitive information for illegal business benefits contrary to the use of the organization's business interest. Account Hijacking and account misuse are other significant threats concerning cloud users. The attacker can impersonate legitimate authorized users to access cloud resources illegally and carry out future malicious activities. Man-In-The-Middle is the act of malicious intruder impersonating legitimate users and positioning themselves in between communication paths to gain unauthorized access to confidential information, conduct unauthorize data manipulation, or even provoke unavailability of service when legitimate employees account is compromised. The attack is possible due to a combination of weak identity, credential, access management vulnerabilities. The absence or presence of a weak encryption algorithm used for data transmitted captured through packet sniffers is also vulnerable. Social Engineering (Phishing, Whaling, Spear phishing, Scam) The act of tricking someone into gaining valuable information from that person legitimately. Users can be exploited through phishing by through scam emails with a malicious attachment or embedded links to a malicious website, through telephone calls to obtain user credentials, or asked to access

a malicious website and put in their credentials which are then recorded for future usage to gain access to the cloud resources. Drive-By Download (Malware Distributor) is a threat where an attacker conducts a stealth download and installation of malicious payload to employee's system without their knowledge when they visit suspicious websites that host malicious contents to prepare the attacker for a future more complex attack. Loss of availability is highly possible due to careless or incompetent system administrators with authorized users with privileged account permissions and little or no knowledge of the required expertise to conduct the task or lack of risk awareness.

Risk Estimation was conducted based on Qualitative Risk Assessment approach using the following variables to Identify Risk around employee(user-id-3) behavior with regards to SaaS resources; Sensitivity of the People-Employees Asset - Qualitative Risk Sensitivity Scale (Derived from User Behavior Trust Degree and User Behavior Risk Rating), Severity or Impact of the Vulnerability - Qualitative Severity/Impact Scale and Likelihood of the Threat - Qualitative Likelihood Scale. An employee with ***user-id_3*** from Table 6 was used as a sample for the risk assessment. The reason was due to the following attributes; Not Credible -User Behavior Trust Degree, High -User Behavior Risk Rating, and High -Sensitivity Rating.

Impact of the Vulnerability - Qualitative Severity/Impact and Likelihood of the Threat -or Qualitative Likelihood, both shown below, were determined for user-id_3 people employee asset. Then, combining these factors to determine the Risk Rating Matrix - Risk Impact- Severity.

Severity or Impact of the Vulnerability: Qualitative Severity/Impact Scale are based on numeric value based on Degree-of negative impact inflicts on organization because of user-id-3 behavior and risk rating

- Financial Loss or revenue
- Legal Implications
- Reputational Damages
- Regulatory Implications

To determine a risk exposure or identified risk for user-id-3, the Qualitative Risk Sensitivity rating in "Table 6: Sensitivity Ratings for "People-Employees" Asset**"** associated to the user behavior trust degree and user risk rating are combined with the above Risk Rating Matrix - Risk Impact- Severity to give a new value of the risk severity impact. Therefore, it is essential to consider a Qualitative Risk Sensitivity rating because it reflects or is associated with parameters "Trust and Risk Rating values" tied to the user-id-3 from the Behavior Trust Evaluation and computation model and behavior risk analysis to determine the actual risk impact

Identified Risk or Estimated Risk Exposure for User-id_3 = [Risk Rating Matrix (impact-Severity) + Qualitative Risk Sensitivity]

The Risk Exposure criteria were used to determine the identified or estimated risk for user-id-3. Risk Sensitivity values were positioned on the top row of the table, while Risk Rating Matrix-

previous impact severity is placed on the lower left bottom of the table. Each intersection of two values determines the new impact severity for the risk. The outcome Risk Estimation process is presented below, an extract from Phase 2*:* Implementing *Trust-Based Adaptive Security Framework based on User Behavior,* as a Risk Mitigation Solution in Risk Management process ISO/2705:2018:

- Impact of the Vulnerability - Qualitative Severity-Impact Scale
- Likelihood of the Threat - Qualitative Likelihood Scale
- Risk Rating Matrix (without with Qualitative Risk Sensitivity) Impact- Severity
- Risk Exposure: (Risk Rating Matrix with Qualitative Risk Sensitivity) Risk Sensitivity

Outcome observation from the risk estimation process proved that the identified or estimated risks for user-id_3 were critical. Taking associated threats, vulnerabilities, impact level, and the likelihood of occurrence into consideration, it reveals a significant insight that users with no-credible trust level and high-risk rating can create or course a very dangerous impact on the well-being of their organization and her valuable asset hosted across the SaaS environment. As a result, users with this profile or category should be given the highest risk treatment priority.

6.2.3 Risk Treatment

After the framework solution was applied to each identified risk as a possible mitigation solution, the user behavior risk sensitivity ratings were reduced one level from High to Low. The primary reason for this reduction was user behavior trust and risk level changes, which affects the risk sensitivity ratings. The occurrence of changes in the risk sensitivity rating was heavily influenced by the application of the corresponding risk treatment or enforcement by the adaptive security control engines. The enforcement of adaptive security controls indeed forced user-id-3 to change their behavior, in addition to recalculating the trust level and associated risk, and further monitored. The new value derived from recalculated behavior trust degree and associated behavior risk rating is used to update the historical trust records and the rest of the processes. Risk assessment is ongoing, so user-id-3 behavior trust and associated risk rating will continuously be monitored and assessed. Inevitably, insight into the current trust state and risk level of the user-id-3 is vital for continuous risk monitoring and updating the user behavior trust list, historical record trust degree, policy decision making, and adaptive security enforcement control.

Risk Register and Risk Monitor are presented in Tables 7 and 8, respectively, with user-id-3's risk treatment mapping, where the precise controls are applied to the corresponding threats, vulnerabilities, and identified risk.

Table 7: Qualitative Risk Assessment - Risk Registry

Risk Register with No Controls								
Asset	Vulnerability	Impact (severity)	Threat	Likelihood	Risk Level without Risk Sensitivity	Risk Sensitivity	Risk Level with Risk Sensitivity Scale	Controls (Adaptive Security Control Engine)
Employee (user-id-3)	Weak Identity, Credential, and access management	High	Account Hijacking and Account Misuse	Certain	Extreme	High	Critical	Preventive Control Process (Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy), Security Policies and Procedure ,Security Awareness Program) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system Retrospective Control Process (Conduct Incident Response) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk, Baselining security posture)
Employee (user-id-3)	Weak Identity, Credential and access management	Medium	Man-In-The-Middle	Possible	High	High	Critical	Preventive Control Process (Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy) ,Security Awareness Program, Implement Encryption Mechanism, Enforce End-Point Security Data Prevention Leakage, Hardening and Isolation, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk, Baselining security posture)
Employee (user-id-3)	Absence or ineffective access control mechanism	High	Malware Infection	Possible	Extreme	High	Critical	Preventive Control Process (Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy), Security Policies and Procedure ,Security Awareness Program, Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies

								identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk, Baselining security posture)
Employee (user-id-3)	Absence or ineffective access control mechanism	Medium	Malicious Insider	Possible	High	High	Critical	Preventive Control Process Enforce Access control Procedures (Multi-Factor Authentication, Complex Password Policy, Security Policies and Procedure ,System Hardening and Isolation, Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Lack of Security Awareness	High	Social Engineering (Phishing, Whaling, Spear phishing, Scam)	Certain	Extreme	High	Critical	Preventive Control Process (Security Awareness Program, Security Policies and Procedure, Enforce Access control Procedures (user accounts),Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Lack of Security Awareness	High	Malware Infection	Likely	Extreme	High	Critical	Preventive Control Process (Security Awareness Program, Security Policies and Procedure,Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage,Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Lack of Security Awareness	Medium	Drive-By Download (Malware Distributor)	Likely	High	High	Critical	Preventive Control Process Security Awareness Program, Security Policies and Procedure, Enforce End-Point Security- Anti-Malware, Content manager, Data Prevention Leakage, Enforce Network Security-IPS, Proxy) Detective Control Process(Logging, real-time monitoring and alerts , Anomalies identification, Intrusion detection system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)

Employee (user-id-3)	Careless or Incompetent System Administrator	Medium	Loss of Service Availability	Possible	High	High	Critical	Preventive Control Process (System Hardening and Isolation, Security Policies and Procedure) Detective Control Process (Logging, real-time monitoring and alerts , system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Careless or Incompetent System Administrator	Catastrophic	Data Breaches and Data Loss	Possible	Extreme	High	Critical	Preventive Control Process (System Hardening and Isolation, Security Policies and Procedure, Enforce End-Point Security Data Prevention Leakage) Detective Control Process (Logging, real-time monitoring and alerts , system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)
Employee (user-id-3)	Improper handling of sensitive	Catastrophic	Data breaches and Data Loss	Possible	Extreme	High	Critical	Preventive Control Process (Security Policies and Procedure, Enforce End-Point Security Data Prevention Leakage) Detective Control Process (Logging, real-time monitoring and alerts , system, incident detection, investigation and contain) Retrospective Control Process (Conduct Incident Response, Change security policy to adapt current situation) Predictive Control Process (Attack Prediction, Risk assessment, Proactive threat intelligence, Foreseen future risk)

Effect of post implemented Adaptive Security Controls and Degraded Risk Sensitivity, as Risk Treatment is presented in Table 8: Risk Register and Risk Monitor.

Table8: Risk Register After Implemented (Adaptive Security Controls) and Degraded Risk Sensitivity - (Risk Monitor)

Asset	Vulnerability	Threat	Impact (severity)	Likelihood	Risk Level without Risk Sensitivity	New Risk Sensitivity	Risk Level with Risk Sensitivity Scale
Employee (user-id-3)	Weak Identity, Credential and access management	Account Hijacking and Account Misuse	Medium	Likely	High	Low	Moderate
Employee (user-id-3)	Weak Identity, Credential and access management	Man-In-The-Middle	Insignificant	Rare	Low	Low	Low
Employee (user-id-3)	Absence or ineffective access control mechanism	Malware Infection	Medium	Unlikely	Moderate	Low	Low
Employee (user-id-3)	Absence or ineffective access control mechanism	Malicious Insider	Low	Unlikely	Low	Low	Low
Employee (user-id-3)	Lack of Security Awareness	Social Engineering (Phishing, Whaling, Spear phishing, Scam)	Medium	Possible	High	Low	Moderate
Employee (user-id-3)	Lack of Security Awareness	Malware Infection	Medium	Possible	High	Low	Moderate
Employee (user-id-3)	Lack of Security Awareness	Drive-By Download (Malware Distributor)	Low	Possible	Moderate	Low	Low
Employee (user-id-3)	Careless or Incompetent System Administrator	Loss of Service Availability	Low	Possible	Moderate	Low	Low
Employee (user-id-3)	Careless or Incompetent System Administrator	Data breaches and Data Loss	High	Unlikely	High	Low	Moderate
Employee (user-id-3)	Improper handling of sensitive	Data breaches and Data Loss	High	Unlikely	High	Low	Moderate

Chapter 7
Discussion

7.1 Summary of Results

This study set out to design a risk mitigation solution known as *User Behavior Trust-Based Adaptive Security framework.* And how it could be used as a possible risk mitigation solution to enhance and resolve users' identity and access control limitations of traditional identity and access management (IAM) during user's interaction with SaaS resources. The findings from this study attempt to answer the research question "How can a trust-based adaptive security framework be integrated into risk mitigation to enhance SaaS user- identity and access control based on user behavior?". It suggests that when a user behavior trust degree, policy decision making, and adaptive security control are integrated into the risk management process, it could mitigate identified risk associated with untrusted user behavior to an acceptable level. After applying the framework as a possible risk treatment, the study demonstrates a possible correlation between reduced risk levels and improved user attitude. This improvement seamlessly led to an increased user behavior trust and lowered behavior risk rating. This study also discusses significant findings on the essential components of the framework(presented in figures 18, 19-a, 19-b, and 20) and its integration into the ISO/2705:2018 risk management process as related to the literature review in chapter 3. In addition to the literature review was the utilization of recognized theoretical concepts and principles to aid the framework's design, due to no study on the research area or underdeveloped area of research concerning the integration of the framework into the risk management process.

The critical functions of design components consisted of; User Behavior Trust Manager that computes a user behavior trust degree and associated risk rating, Policy Decision Point (PDP) central, that adapt and set each user trust and risk levels through logical processing into the following categories; “Complete Trust, Partial Trust, and Not Credible” and “High, Medium, and Low-risk ratings.” These adapted values from PDP, later used as the key parameters when determining the access control decision classified as "Grant full access, Grant limited access, or Deny access." Depending on the resulting decision, the Adaptive Security Control Engine conducts a security controls enforcement that could be preventive, detective, corrective or predictive, corresponding to a specific user behavior trust level.

One of the most significant outcomes of the result was that identified risk caused by untrusted user behavior presented in Table 7, *Qualitative Risk Assessment - Risk Registry,* was reduced to an acceptable level after the framework was applied as a possible risk treatment, shown in Table 8 *Risk Register and Risk Monitor*. As previously expressed, changes in the user behavior to a more trusted one with a low-risk rating possibly influenced the risk reduction. This effect might significantly enhance the user identity and access control management across SaaS environments.

The risk management process was conducted by selecting a sample of people assets identified as employee-id tagged with "User-id-3" from the asset identification and valuation phase. User-id-3 was prioritized for risk treatment due to the following profile; user behavior trust level of "not credible," and user behavior risk rating of "high" with asset valuation sensitivity rating of "high." The framework solution and its integration into the ISO/2705:2018 risk management process are described in detail in the following sections. The study further outlines implications of the framework as a possible risk treatment solution and limitations of the study.

7.2 Results Interpretation: The Designed Framework & ISO/2705:2018 Risk Management Process

7.2.1 User Behavior Trust Manager

As previously expressed in chapters 5, 6, and figure 20, the user behavior trust manager is a crucial component of the framework, where its key elements function collectively to produce a well-functioning trust evaluation capability. These fundamental elements were behavior trust evidence collector, Interactive user collector, risk assessment process, trust and risk databases, and trust evaluation modeling engine.

The evaluation trust model computes the user behavior trust level known as comprehensive trust degree and associated risk rating from a combination of previously defined trust parameters such as recommended trust, direct trust, and historical trust with a weighted constant value. These previously derived trust types were formulated based on evidence from recommendations of users' interaction, historical records, and user activities in the form of different logs types of data sources across the cloud. These logs of various origins were parsed, correlated, and analyzed to create a user behavior trust profile that is later fed into the trust evaluation model to determine the users' trust state and risk levels and finally derived the user trust behavior level and associated risk rating.

The resulting data from the user behavior trust manager, comprising of; the user behavior comprehensive trust degree and associated risk rating were used and contributed to the access control decision-making by the Policy Decision Point central server, which is then fed finally into an Adaptive Security Control Engine that enforced the access control decision. This resulting data from the User Behavior Trust Manager were used by the Policy Decision Point to formulate the User-id-3 sample profile; user behavior trust level of "not credible," and behavior risk rating of "high." In conjunction with asset valuation sensitivity rating of "high.". This same resulting data played a significant role as the primary link and parameters between the Asset Identification and Valuation phase when conducting ISO/IEC 27005:2018 Risk Assessment process. Table 6-Sensitivity Ratings for People-Employees Asset presented the primary link and parameters to the

Risk Assessment process. It might provide a clearer understanding of how the user trust behavior and associated risk rating can be integrated into the entire ISO/IEC 27005:2018 Risk Management process. The resulting outcome was a likely relationship established and aligned with the risk management process. In reviewing the literature, no data was found on the association between user behavior trust degree & associated behavior risk rating and the risk management process from previous research. This possible association established in the results facilitates the traceability of specific user behavior to the risk assessment- people employees as an asset and the corresponding risk treatment for the cloud's remediation process. The increased behavior trust and reduced risk rating reflected the positive changes of user-id-3 attitude after post risk treatment and further used to update the historical trust records and the rest of the processes for continuous risk monitoring

Prior studies have noted the importance of user behavior trust as a mechanism to support the authentication process since it is not enough to provide sufficient security across the cloud. However, for this view to be possible, a Trust Evaluation model needed to be designed based on the seven principles for evaluating users according to [69] research work, *User Behavior and Trust Evaluation in Cloud Computing*. Furthermore, as mentioned in the literature review in chapter 3 concerning a selection of an appropriate trust evaluation model from the comparison between different trust models [69], the *Trust evaluation model of cloud users based on behavior data* was selected and adapted as a choice of a trust evaluation and computation engine [74]. The ability of the adapted trust evaluation model to apply its algorithms in conjunction with the seven principles for evaluating users during modeling user trust of how they utilize the cloud was significant criteria over other important trust models such as Fuzzy Adaptive Resonance Theory (ART) and Neuro-Fuzzy Techniques [73].

Although recent research has suggested that integrating a trust-based concept into adaptive security will ensure a secure, ubiquitous computing environment [16], the researchers did not provide any practical guide to how this could be implemented. Further research *Trust-based decision-making for smart and adaptive environments, User Modeling and User-Adapted Interaction*, conducted by [54], also suggested trust-based decision-making for smart and adaptive environments based on Bayesian networks' User Trust Model, ensuring users' experience and acceptance of smart energy systems. However, the trust perspective was based on how users perceived and accepted the smart system but not putting user behavior into context and influencing the adaptive nature of the smart energy system. Additional interesting research, *Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes' Recommendations for WSN* by [66], outlined trust management as a critical factor that will evaluate and establish trustworthy nodes during packet routing across the node and thereby choosing a node for routing across Wireless Sensor Network also detecting their unexpected node behavior. An alternative mechanism instead of routing packets in the encrypted format against eavesdropping. The [66] research was tailored towards WSN nodes instead of user activities and related behavior. A similar study, *TAS-IoT: Trust-Based Adaptive Security in the IoT* by [68], emphasizes the significance of integrating the

concept of trust to adaptive security that considerably reduces energy consumption across IoT nodes and remains secure. The research work by [68] was based on the IoT node trust context and its adaptivity. The closest related work regarding user behavior was the *Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security*" by the researcher [75]. The main objective was to analyze human behavior and determine its behavioral trust degree through the Fuzzy-logic trust model, which forms the basis for an adaptive security policy [75]. But the research did not consider the effect and impact of integrating a user behavior trust into the ISO/2705:2018 Risk Management process to help determine or link to an adaptive security policy; in other words, adaptive security preventive control.

7.2.2 Policy Decision Point (PDP) Central Server

The Policy Decision Point shown in figures 19-a & 19-b is one of the vital components of the designed framework. Its primary function is to process and generate additional user behavior trust and risk rating parameters that will be further mapped into a decision-making process.

The Logical processor presented in figure 19-b takes in the resulting user behavior comprehensive trust degree and then evaluates it against an Abnormal Threshold value plus associated user behavior risk rating. Afterward, adapts and set each user's trust and risk levels, categorized as Complete Trust, Partial Trust, and Not Credible, and risk rating of High, Medium, and Low Risk. The process makes these values suitable for the decision-making process. Based on the newly adapted and set parameters, the decision-making process dictates the following access control "Grant full access," "Grant limited access, or "Deny Access," depending on resulting user trust and risk levels derived previously. An adaptive security engine later enforces the outcome access control decision. An example of the resulting data from the PDP was the user-id-3 with the following profile; user behavior trust level of "not credible," and user behavior risk rating of "high" with access control decision of "deny access." As expressed previously, the same resulting data played a significant role as the primary link and parameters when conducting ISO/IEC 27005:2018 Risk Assessment, as presented in Table 6.

While previous research has focused on eXtensible Access Control Markup Language as the only standardized access control standard that dynamically enforces authorization for resource access [79], the idea of adapting this standardized protocol to create a modular user identity and access control management across the cloud might be significant. The process involved integrating the policy decision point to process the user behavior trust degree and associated risk rating for access decision making in conjunction with access control enforcement by the adaptive security control.

7.2.3 Adaptive Security Control Engine

Also expressed previously in chapters 5, 6, and presented in figure 18, the adaptive security control engines function as control enforcement points. The system dynamically enforces any four controls as part of its risk treatment capabilities: preventive, detective, retrospective, or respond, and predictive controls based on the type of decision received as input from the Policy Decision Point.

The received decisions are associated with each user behavior trust level and associated risk rating, which is then subjected to adaptive and adynamic security enforcement to mitigate the actual threat and identified risk. Figure 18 presents the critical elements within the preventive, detective, retrospective, or respond and predictive controls. The controls were applied as a part of the risk treatment and a continuous risk management process that might enhance cloud users' identity and access control management. For example, the effect of applying the adaptive security control engine as a risk treatment could be observed through a user tagged with a user-id-3 with associated profile; user behavior trust level "not credible," user behavior risk rating "high," with access control decision "deny access.". The adaptive security controls reduced each identified risk related to user-id-3 attitude or behavior to one level lower m as observed in Table 8, Risk Register and Risk Monitor. A reasonable explanation for this reduction was due to changes in the user attitude, which eventually led to an increase in user behavior trust level and seamless decrease of the behavior risk rating after the adaptive security controls were applied as risk treatment.

Incorporating the adaptive security control as part of the framework with its resulting outcome was built on the existing principle and concept *Designing an Adaptive Security Architecture for Protection From Advanced Attacks* by [78], to design a security control that can dynamically adapt to ubiquitous environments like the cloud and IoT against emerging threats. [78] principle and concept have been widely accepted and applied in the information security field of studies. Although, despite the widely accepted principles and concepts by [78], which constitute the fundamental aspect of the system, the idea of associating it to the policy decision point and the user trust level with behavior risk rating was a significant idea that might help focus on tackling and treating identified risk exclusive related to people as an asset during the risk management process.

Previous research that relied on [78] principle and the concept was the research studies *Adaptive Security Framework for the Blockchain on IoT,* conducted by [12], a framework designed to dynamically compute and allocate existing resources for IoT nodes while maintaining a secure environment. However,[12] did not tailor the research towards a user behavior trust context; instead, it focuses on the interaction of the IoT nodes to adaptively compute and allocate resources during blockchain processing. In addition, research work *Adaptive Risk Management Framework for Cloud Computing* by [63] emphasized implementing a dynamical risk treatment framework over a statically approach balance between the security and performance degradation.

However, the implementation of the security mechanism fell short of applying this approach to a user behavior trust context since user behavior trust context was not the key focus of the research risk management framework. Lastly, [64] research adapted the adaptive security principle and concept to design *Risk-Based Adaptive Security for Smart IoT in eHealth* to estimate and predict risk damages and future benefits using game theory and context-awareness techniques. However, [64] did not tailor the research towards a user behavior trust context since it was not a key focus.

7.2.4 ISO/2705:2018 Risk Management Process

This section outlines the resulting outcome of the risk assessment and treatment processes, detailing how the designed framework was integrated and used as a possible mitigation solution that might help resolve identified risks associated directly with untrusted user behavior. The process started by defining a context with employees classified as people assets presented in Tables 4 and 6. Afterward, risk sensitivity rating was used as a critical factor to determine how valuable or essential people asset was. Next, the people asset was identified as User-id-3, later used as a sample during the risk management. Finally, User-id-3 was prioritized for risk treatment due to the following profile: user behavior trust level "not credible," user behavior risk rating "high" with asset valuation rating "high sensitivity.". As mentioned previously, User-id-3 with an associated profile formed a likely primary link and parameters that could be regarded as a relationship between the designed framework and the ISO/IEC 27005:2018 Risk management process, as presented in Tables 6, 7, and 8. The likely established relationship between the "designed framework and the ISO/IEC 27005:2018 Risk management process ", in conjunction with the combination of the following theoretical concept of; user behavior trust manager, policy detection, and adaptive security control, might be considered as the underlining factor that makes this project probably unique beyond the state-of-the-act. Next were the Risk Assessment and Risk Treatment processes outlined in the subsequent sections.

The Risk Assessment process was performed using sample User-id-3 that was prioritized for risk treatment due to its associated profile and potential to inflict severe damage to the cloud service. As a result, the identified risk was directly associated with any users, as presented in Table 7 *Qualitative Risk Assessment - Risk Registry*. The Qualitative risk assessment approach identified the resulting identified risk by combining the initially derived risk matrix, then combined with the risk sensitivity scale to form a more granular matrix to determine the identified risk ultimately. Afterward, the framework was applied to each identified risk directly related to the User-id-3 profile during the Risk Treatment process as presented in Table 8, *Risk Register and Risk Monitor*. As a result, the user behavior risk sensitivity ratings were reduced from High to Low. The primary reason for reducing associated risk with User-id-3 changed to the user attitudes or behavior as expressed previously, eventually affecting the risk sensitivity ratings, which might have influenced the risk ratings. Therefore, the positive changes of user-id-3 were reflected in the user's increased behavior trust value and reduced behavior risk rating. This data

formed the basis for updating the historical trust records and the rest of the processes for continuous risk monitoring.

7.3 Practical Implications of the Designed Framework

This combination of findings supports the conceptual premise that the *Trust-Based Adaptive Security Framework based on User Behavior* could be adapted and used as possible guidelines or recommendations for the research community and information security field of study to help enhance user identity and access control management across the SaaS. Furthermore, the evidence from this study suggests that when cloud user activities with associated behavior trust levels are analyzed and monitored during an attempt to bypass any access controls or after being granted access, could help give an insight into the security posture of the cloud environment, and enforced the corresponding control measure to remediate risk through the ISO/IEC 27017:2015 Risk Management process.

However, referring back to the literature review, Traditional Cloud User Entity and Access Control mechanisms such as; Identity and Access Management (IAM), Identity-as-a-Service (IDaaS), and Cloud Identity Management [23] were known to show weakness when tracking a particular user to specific activities. An example of this limitation could be that cloud users constantly move across domain network infrastructure, seamlessly changing between IP addresses, assets, and clouds services; tracking down malicious user activities tends to be complicated. Another example is; that a malicious actor might masquerade and infiltrate the corporate network due to compromised legitimate users to conduct malicious activities that might go undetected.

From an information security standpoint and referring to the literature review, the ISO/IEC 27017:2015 Risk Management process did not explicitly dictate how People Asset should be defined during the Context definition and Risk Assessment phase [29]. As a result, the idea of integrating the "User Behavior Trust context" as a People Asset into the ISO/IEC 27017:2015 Risk Management process could be a reasonable approach that might help focus exclusively on tackling identified risks directly associated with users activities or attitudes across the cloud. Eventually, this approach might enhance how user identity and access control are effectively managed across the cloud.

7.4 Limitations of the Research

Among the limitations faced with the thesis project was simulating a trust modeling processor, policy detection point server, and adaptive security engines to produce a proof of concept to

support the research finds. Moreover, the possibility of finding an appropriate open-source software with integrated Artificial intelligence to simulate the adaptive security architecture with corresponding subsystems control engines was not possible; most existing adaptive security architecture are built-in cyber security platforms as a proprietary product. In addition, processors for simulating a user behavior trust-modeling, in conjunction with eXtensible Access Control Markup Language were additional challenges experienced. In general, the lack of adequate resources limited the ability to present a clear picture through a proof of concept of how the technologies, concepts, and principles function collectively to produce the outlined result. Furthermore, risk Monitoring and Risk Communication were exempted from the complete Risk Management process due to the project's scope.

Despite these limitations of the research outlined previously, the findings or results reported for the design and implementation appear to support the assumption that when the designed framework is integrated into the Risk Management process, it might reduce risk to an acceptable. For example, identified risks directly related to untrusted user behavior during interaction with the cloud environment. Furthermore, seamlessly enhancing user identity and access control management of traditional identity and access control mechanism that relies exclusively on user-assigned IP addresses that are prone to changes as users move from domain to domain across the cloud with a specific user account, instead of taking into consideration the behavior of the user and associated activities behind that account.

Chapter 8
Conclusion and Future Research Directions

8.1 Conclusion

The research project aimed to develop a risk mitigation solution known as *User Behavior Trust-Based Adaptive Security framework* that would attempt to answer the research question:" How can a trust-based adaptive security framework be integrated into risk mitigation to enhance SaaS user identity and access control based on user behavior?". A framework that will be specifically based on user behavior trust context and how it can be integrated into the ISO/2705:2018 risk management process to possibly enhance the limitations of traditional User Identity and Access Control management solutions during users' interaction with the SaaS cloud environment. The significant resulting outcome of this study shows that when a user behavior trust degree or trust level, policy decision making, with an adaptive security control is integrated into the risk management process, it could mitigate or reduce the risk associated with untrusted user behavior to an acceptable risk level during the user interaction with the cloud. Furthermore, it demonstrates a possible correlation between the reduced risk level and improved user attitude. An effect that eventually increased a user behavior trust level and seamless reduction of associated behavior risk rating after implementing the framework as risk treatment during ISO/2705:2018 risk management process.

A Trust evaluation model that evaluates users' behavior based on their activities was integrated with a policy decision point and an adaptive security control processor. The user behavior trust model generates the trust level and associated risk rating based on how they behave before and after granting access. Individual trust levels can be increased or decreased by punishment based on the current attitude of the user. The policy decision point concept included in the design was to provide a logical decision-making point that the adaptive security process will consult. The function of the adaptive security processes is to enforce the corresponding controls to mitigate the risk caused by the user actions. Implementing the design framework into the risk management process as a possible treatment solution for identified risk exposure did show how the risk exposure level was reduced and user risk sensitivity level that is tightly liked to both; behavior trust level and behavior risk level. The primary reason for the reduction was due to controls enforced by the adaptive security processor, which might have influenced the user behavior and eventually reduced the risk level. The change in attitude also affected the recalculation of the behavior trust degree and behavior risk ratings and are reflected as an update to the historical trust degree records. In the background, the design framework was conceptually based by illustrating how behavior trust modeling can be integrated into security features such as policy decision point and adaptive security to produce a possible risk mitigation solution to

resolve limitations and enhance the implementation of user identity and access control mechanism across the cloud environment.

While the design is still not conclusive in real-world practicality or implications, it can still be suggested that the resulting framework could still be useful or improved by other researchers in the research community and information security field of study for SaaS. The framework was designed based on combinations of proven technological or scientific concepts and principles such as; user behavior trust modeling, adaptive security architecture, and eXtensible access control markup language, with its integration into a standard ISO/2705:2018 risk management process.

The core functionality is to uniquely identify, control and monitor access based on a user behavior pattern from individual activities. Conventional methods of controlling access after users are successfully identified and granted access are insufficient enough because a legitimate authorized user account can be exploited due to vulnerabilities, for example, abuse of user account or credential theft, to name a few. This shortcoming of uniquely and continuous monitoring of users trying to access the cloud illegally or even legitimate users with malicious intent should still be monitored and controlled through user behavior trust and associated risk levels within the cloud environment since humans are the weakest link in the security chain. Based on the rationale of the framework's core functionality, the notion that the *Trust-Based Adaptive Security Framework* based on “User Behavior Trust context “could serve as a recommended guideline to the research community and information security field of study to contribute to the enhancement of cloud user identity and access control management is the ultimate goal of the project.

8.2 Future Research Directions

The research was based on a conceptual and abstract presentation of how scientific research and technological concepts and principles can be put together to produce a framework solution that might be applicable in the real world. However, due to the limitations faced with this thesis project, with regards to the ability to simulate the framework system functionalities to provide a proof of concept, a sample result of the research finds, and its real-world implication. Therefore, I suggest that further research be undertaken to establish the viability or practicability of the designed framework. That would involve simulating and transforming this conceptual and abstract framework into a real-world working solution for the benefits of the information security field of practice and the research community. Additional suggested research area, "Trust-based adaptive security focusing exclusively on services and applications-processes behavior," might be an area of interest that will focus specifically on services and applications-processes behavior trust context to possibly contribute to the enhancement of computing processes identity and access control management within the SaaS environment.

References

[1] K. Costello and M. Rimol, "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020", *Gartner*, 2020. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020.

[2] R. Mogull, J. Arlen, A. Lane, G. Peterson, M. Rothman, and D. Mortman, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, 4th ed. Cloud Security Alliance, 2017, pp. 7-9.

[3] F. Liu, J. Mao, R. B. Bohn, J. V. Messina, M. L. Badger, and D. M. Leaf, *NIST Cloud Computing Reference Architecture, NIST special publication 500-292*. Gaithersburg, MD: National Institute of Standards and Technology, 2011, pp. 1-28.

[4] J. Brook, D. Shackleford, V. Hargrave, H. Jameson, and M. Roza, *The Treacherous Twelve' Cloud Computing Top Threats in 2016*. Cloud Security Alliance, 2016, pp. 9-35.

[5] A. van der Stock, B. Glas, N. Smithline and T. Gigler, "OWASP Top Ten Web Application Security Risks | OWASP," *Owasp.org*, 2017. [Online]. Available: https://owasp.org/www-project-top-ten/.

[6] M. Whitman and H. Mattord, *Management of information security*, 6th ed. Cengage Learning, 2018, pp. 314,374.

[7] H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in eHealth," *In Proceedings of the 7th International Conference on Body Area Networks*, pp. 269-275, 2012. Available: https://www.balasingham.net/Content/files/pdf/publication-aAdtraMh52EABeSo52gOXijpGVQNfFYSTheFGXv3.pdf.

[8]W. Aman, "Human Aspects of Information Security, Privacy, and Trust," *Lecture Notes in Computer Science*, vol. 9750, pp. 201-211, 2016. Available: https://link.springer.com/chapter/10.1007/978-3-319-39381-0_18.

[9] G. Jagadamba and B. Babu, "Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment: A Comprehensive Survey," *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 1-7, 2016. Available: https://www.researchgate.net/publication/313411800_Adaptive_Security_Schemes_based_on_Context_and_Trust_for_Ubiquitous_Computing_Environment_A_Comprehensive_Survey.

[10]T. El-Maliki, N. Abdennadher, and M. Bouchedakh, "Adaptive security in cloud and edge networks: new IoT security approach," *Proceedings of the 13th International Conference on Systems, ICONS 2018, 22-26 April 2018, Athens, Greece*, pp. 22-26, 2018.

[11] H. Abie, R. Savola, and J. Bigham, "Self-Healing and Secure Adaptive Messaging Middleware for Business-Critical Systems," *International Journal on Advances in Security*, vol. 3, no. 1 & 2, pp. 34-51, 2010.

[12] V. Methane and P. Lakshmi, "Adaptive Security Framework for the Blockchain on IoT," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 9, pp. 3327-3331, 2019. Available: https://www.ijitee.org/wp-content/uploads/papers/v8i9/I9009078919.pdf.

[13] D. Kim and M. Vouk, "A survey of common security vulnerabilities and corresponding countermeasures for SaaS," *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 59-63, 2014. Available: https://ieeexplore.ieee.org/abstract/document/7063386.

[14] Rob van der Meulen, G., 2017. *Build Adaptive Security Architecture Into Your Organization*. [online] Gartner. Available at: <https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization>.

[15] Rob van der Meulen, G., 2017. *The Four Stages of an Adaptive Security Architecture*.[online] Gartner. Available at: <https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization>.

[16] G. Jagadamba and B. Babu, "Adaptive Security Schemes based on Context and Trust for Ubiquitous Computing Environment: A Comprehensive Survey," *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 7-14, 2016. Available: https://www.researchgate.net/publication/313411800_Adaptive_Security_Schemes_based_on_Context_and_Trust_for_Ubiquitous_Computing_Environment_A_Comprehensive_Survey.

[17]A. Singh and K. Chatterjee, "A multi-dimensional trust and reputation calculation model for cloud computing environments," *2017 ISEA Asia Security and Privacy (ISEASP)*, 2017. Available: https://ieeexplore.ieee.org/document/7976983.

[18]A. Gholami and M. Arani, "A Trust Model Based on Quality of Service in Cloud Computing Environment," *International Journal of Database Theory and Application*, vol. 8, no. 5, pp. 161-170, 2015. Available: 10.14257/ijdta.2015.8.5.13.

[19]Q. Sheng, X. Qiao, A. Vasilakos, C. Szabo, S. Bourne, and X. Xu, "Web services composition: A decade's overview," *Information Sciences*, vol. 280, pp. 218-238, 2014. Available: 10.1016/j.ins.2014.04.054.

[20]H. Haas and A. Brown, "Web Services Glossary," *W3.org*, 2004. [Online]. Available: http://www.w3.org/TR/ws-gloss/.

[21] D. Benslimane, S. Dustdar, and A. Sheth, "Services Mashups: The New Generation of Web Applications," *IEEE Internet Computing*, vol. 12, no. 5, pp. 13-15, 2008. Available: 10.1109/mic.2008.110.

[22] "Web service - Wikipedia", *En.wikipedia.org*, 2017. [Online]. Available: https://en.wikipedia.org/wiki/Web_service.

[23]D. Sharma, C. Dhote and M. Potty, "Identity and Access Management as Security-as-a-Service from Clouds," *Procedia Computer Science*, vol. 79, pp. 170-174, 2016. Available: https://www.sciencedirect.com/science/article/pii/S1877050916002489.

[24] W. Denniss, J. Bradley, "OAuth 2.0 for Native Apps", Tech. Rep. RFC 8252, Internet Engineering Task Force (IETF), 2017. Available: URL https://tools.ietf.org/html/rfc8252.

[25] Docs.oasis-open.org, "Web Services Security: SOAP Message Security 1.1", *Oasis-open.org*, 2004. [Online]. Available: https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf..

[26]"WS-Security - Wikipedia", *En.wikipedia.org*, 2016. [Online]. Available: https://en.wikipedia.org/wiki/WS-Security.

[27]Docs.oasis-open.org," Web Services Federation Language (WS-Federation) Version 1.2", *Oasis-open.org*, 2009. [Online]. Available: http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html.

[28]S. Hammer, M. Wißner and E. André, "Trust-based decision-making for smart and adaptive environments," *User Modeling and User-Adapted Interaction*, vol. 25, no. 3, pp. 267-293, 2015. Available: 10.1007/s11257-015-9160-8.

[29] D.Ionita & P.Hartel, W.Pieters, and R.Wieringa ."The ISO 27005 Risk Management workflow", *Current Established Risk Assessment Methodologies and Tools*. (2014). Available:10.13140/RG.2.2.22914.68806.

[30] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final.

[31]"ISO/IEC 17788:2014", *ISO/IEC 17788:2014(en) Information technology — Cloud computing — Overview and vocabulary*, 2014. [Online]. Available: https://www.iso.org/standard/60544.html.

[32] R. Mogull, J. Arlen, A. Lane, G. Peterson, M. Rothman, and D. Mortman, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, 4th ed. Cloud Security Alliance, 2017, pp. 10 -20.

[33] R. Mogull, J. Arlen, A. Lane, G. Peterson, M. Rothman, and D. Mortman," Essential characteristics of cloud computing, "*Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*, 4th ed. Cloud Security Alliance, 2017, pp. 10-30.

[34]F. Liu et al., "NIST Cloud Computing Reference Architecture," *NIST*, 2011. [Online]. Available: https://www.nist.gov/publications/nist-cloud-computing-reference-architecture.

[35]"Shared Responsibility Model Explained", *CloudPassage*, 2020. [Online]. Available: https://www.cloudpassage.com/articles/shared-responsibility-model-explained/.

[36]T. Erl, Z. Mahmood, and R. Puttini, *Cloud computing*, 1st ed. Upper Saddle River: Prentice-Hall, 2014, pp. 79-113.

[37] S. Carlin and K. Curran, "Cloud Computing Technologies," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, vol. 1, no. 2, pp. 59-63, 2012. Available: 10.11591/closer.v1i2.486.

[38]A. Shawish and M. Salama, "Cloud Computing: Paradigms and Technologies," *Inter-cooperative Collective Intelligence: Techniques and Applications*, pp. 39-67, 2013. Available: https://link.springer.com/chapter/10.1007%2F978-3-642-35016-0_2.

[39]"Web Applications | Arcitura Patterns", *Patterns.arcitura.com*, 2018. [Online]. Available: https://patterns.arcitura.com/cloud-computing-patterns/basics/web-technology/web_applications.

[40] M.Payal & M.Upadhyay, D.Mathur, and T.Sharma. A STUDY OF CLOUD DESIGN MODEL WITH RESPECT TO PARALLEL AND DISTRIBUTED NETWORK FOR EFFICIENT APPLICATION.1-2018. (2018)

[41] L. Evensen, "Using the cloud for business continuity - Cloud computing news," *Cloud computing news*, 2014. [Online]. Available: https://www.ibm.com/blogs/cloud-computing/2014/09/04/using-cloud-business-continuity/.

[42] C. Orieschnig, "The 10 Best SaaS Companies (2021)", *PakWired*, 2021. [Online]. Available: https://pakwired.com/best-saas-companies/.

[43]"Software as a Service | SAAS", *Thedeveloperblog.com*, 2018. [Online]. Available: https://thedeveloperblog.com/software/software-as-a-service.

[44] "Software as a service - Wikipedia," *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Software_as_a_service.

[45] "Definition of Identity and Access Management (IAM) - Gartner Information Technology Glossary," *Gartner*, 2020. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam.

[46] G. Keller, "What is Cloud Identity Management? - JumpCloud", *JumpCloud*, 2021. [Online]. Available: https://jumpcloud.com/blog/what-is-cloud-identity-management/.

[47] *SecaaS Defined categories of service 2011*, 1st ed. Cloud Security Alliance., 2011, pp. 7-21.

[48] *SecaaS Implementation Guidance, Category 1: Identity and Access Management*, 1st ed. Cloud Security Alliance, 2012, pp. 10-14.

[49] A. Chaudhary, "Cloud Security Challenges in 2020", *Cloudsecurityalliance.org*, 2020. [Online]. Available: https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020/.

[50] C. Dellarocas, "The Digitization of Word of Mouth: Promise and Challenges of Online Feedback Mechanisms," *Management Science*, vol. 49, no. 10, pp. 1407-1424, 2003. Available: 10.1287/mnsc.49.10.1407.17308.

[51] D. Romano, "The nature of trust: Conceptual and operational clarification," Ph.D., Louisiana State University and Agricultural & Mechanical College, 2003.

[52] B. Barber and D. Gambetta, "Trust: Making and Breaking Cooperative Relations.", *Contemporary Sociology*, vol. 21, no. 3, p. 401, 1992. Available: 10.2307/2076328.

[53] S. Marsh, "Formalizing Trust as a Computational Concept," Ph.D., University of Stirling, Department of Computer Science and Mathematics, 1994.

[54] S. Hammer, M. Wißner and E. André, "Trust-based decision-making for smart and adaptive environments," *User Modeling and User-Adapted Interaction*, vol. 25, no. 3, pp. 267-293, 2015. Available: 10.1007/s11257-015-9160-8.

[55]"What Is User and Entity Behavior Analytics (UEBA)?", *Rapid7*, 2020. [Online]. Available: https://www.rapid7.com/fundamentals/user-behavior-analytics/.

[56] D. Gough, S. Oliver, and J. Thomas, *An introduction to systematic reviews*, 2nd ed. London: SAGE Publications Ltd, 2017, pp. 10-30.

[57] C. Okoli, "A Guide to Conducting a Standalone Systematic Literature Review," *Communications of the Association for Information Systems*, vol. 37, no. 43, pp. 3-28, 2015. Available: 10.17705/1cais.03743.

[58] C. Kothari, *Research methodology*, 2nd ed. New Delhi: New Age International, 2004, pp. 1-15.

[59] M. Saunders, P. Lewis, and A. Thornhill, *Research methods for business students*, 8th ed. Harlow: Pearson Education Limited, 2019, pp. 128-170.

[60] A. Bryman, *Social Research Methods - 5th Edition*, 5th ed. Oxford: OXFORD University Press, 2016, pp. 200-220.

[61] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities, and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1-48, 2019. Available: 10.1016/j.cosrev.2019.05.002.

[62] O. Ali, A. Shrestha, A. Chatfield, and P. Murray, "Assessing information security risks in the cloud: A case study of Australian local government authorities," *Government Information Quarterly*, vol. 37, no. 1, p. 101419, 2020. Available: 10.1016/j.giq.2019.101419.

[63] M. Medhioub, M. Hamdi and T. Kim, "Adaptive Risk Management Framework for Cloud Computing," *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, pp. 1154-1161, 2017. Available: 10.1109/aina.2017.143.

[64] H. Abie and I. Balasingham, "Risk-Based Adaptive Security for Smart IoT in eHealth," *Proceedings of the 7th International Conference on Body Area Networks*, pp. 269-275, 2012. Available: 10.4108/icst.bodynets.2012.250235.

[65]W. LI, T. JIANG, Y. YUAN, and Z. DI, "Hybrid Trust Chain Security Model with Cloud Computing Based on Smart Grid," *DEStech Transactions on Computer Science and Engineering*, no., 2017. Available: 10.12783/dtcse/cst2017/12519.

[66] S. Babu, A. Raha, and M. Naskar, "Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes' Recommendations for WSN," *Wireless Sensor Network*, vol. 06, no. 08, pp. 157-172, 2014. Available: 10.4236/wsn.2014.68016.

[67] J. Huang and D. Nicol, "Trust mechanisms for cloud computing," *Journal of Cloud Computing: Advances, Systems, and Applications*, vol. 2, no. 1, p. 9, 2013. Available: 10.1186/2192-113x-2-9.

[68]H. Hellaoui, A. Bouabdallah, and M. Koudil, "TAS-IoT: Trust-Based Adaptive Security in the IoT," *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, pp. 599-602, 2016. Available: 10.1109/lcn.2016.101.

[69] M. Alruwaythi, K. Kambampaty, and K. Nygard, "User Behavior and Trust Evaluation in Cloud Computing," *Proceedings of 34th International Conference on Computers and Their Applications*, vol. 58, pp. 378{386, 2019.

[70] L. Jun-Jian and T. Li-Qin, "User's Behavior Trust Evaluate Algorithm Based on Cloud Model," *2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC)*, pp. 556-561, 2015. Available: 10.1109/imccc.2015.123.

[71] J. Ma and Y. Zhang, "Research on Trusted Evaluation Method of User Behavior Based on AHP Algorithm," *2015 7th International Conference on Information Technology in Medicine and Education (ITME)*, pp. 588-592, 2015. Available: 10.1109/itme.2015.39.

[72] R. Yang and X. Yu, "Research on a way of evaluating cloud end-user behavior's credibility based on the methodology of multilevel fuzzy comprehensive evaluation," *Proceedings of the 6th International Conference on Software and Computer Applications - ICSCA '17*, pp. 165–170, 2017. Available: 10.1145/3056662.3056677.

[73] M. Jaiganesh, M. Aarthi, and A. Vincent Antony Kumar, "Fuzzy ART-Based User Behavior Trust in Cloud Computing," *Advances in Intelligent Systems and Computing*, pp. 341-348, 2014. Available: 10.1007/978-81-322-2126-5_38.

[74] Z. Chen, L. Tian and C. Lin, "Trust evaluation model of cloud user based on behavior data," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, p. 155014771877692, 2018. Available: 10.1177/1550147718776924.

[75] I. Brosso and A. La, "Adaptive Security Policy Using User Behavior Analysis and Human Elements of Information Security," *Fuzzy Logic - Emerging Technologies and Applications*, 2012. Available: 10.5772/36079.

[76] I. Bica, B. Chifor, Ș. Arseni and I. Matei, "Reputation-Based Security Framework for Internet of Things," *Innovative Security Solutions for Information Technology and Communications*, pp. 213-226, 2020. Available: 10.1007/978-3-030-41025-4_14.

[77] D. Silverman, *Doing qualitative research*. Thousand Oaks, CA: Sage Publications, 2013.

[78] N. MacDonald and P. Firstbrook, "Designing an Adaptive Security Architecture for Protection From Advanced Attacks," *Gartner*, 2014. [Online]. Available: https://www.gartner.com/en/documents/2665515/designing-an-adaptive-security-architecture-for-protecti.

[79] B. Parducci and H. Lockhart, "OASIS eXtensible Access Control Markup Language (XACML) TC | OASIS," *Oasis-open.org*, 2011. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[80] I. Indu, P. Anand, and V. Bhaskar, "Identity and access management in a cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574-588, 2018. Available: 10.1016/j.jestch.2018.05.010.

[81] Atta-ur-Rahman, S. Dash, A. Luhach, N. Chilamkurti, S. Baek and Y. Nam, "A Neuro-fuzzy approach for user behaviour classification and prediction," *Journal of Cloud Computing*, vol. 8, no. 1, pp. 1-15, 2019. Available: 10.1186/s13677-019-0144-9.

[82] E. Wheeler, *Security risk management*, 1st ed. Waltham, MA: Syngress, 2011, pp. 3-160.

[83] M. Lundgren, *Risk identification, Monitoring, and Analysis*. Luleå Sweden: Master Programme in Information Security, Luleå University of Technology, 2019, pp. 1-29.