

11-25-2025

The Impact of Machine Learning Security Models on Cloud Data Security

Ali Sanad
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Ali Sanad

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Nawaz Khan, Committee Chairperson, Information Technology Faculty
Dr. Constance Blanson, Committee Member, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2025

Abstract

The Impact of Machine Learning Security Models on Cloud Data Security

by

Ali Sanad

MS, Walden University, 2022

BS, Colorado State University, 2019

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

October 2025

Abstract

Many information technology (IT) leaders face challenges in adopting machine learning (ML) models for cloud infrastructure, despite their potential to enhance data security. The extent to which IT leaders' perceived security (PeS) and perceived privacy (PeP) influence their intent to adopt ML security models is critical for organizational success. Grounded in the technology acceptance model, the purpose of this quantitative correlational study was to examine the relationship between IT leaders' PeS and PeP and their intent to adopt ML security models in cloud-based applications. Data were collected from 106 IT professionals in Chicago using a validated instrument. Results from a hierarchical multiple regression analysis indicated that PeS and PeP jointly explained a significant proportion of variance in the intent to adopt ML models ($R^2 = .536$, $F(8, 97) = 14.01$, $p < .001$). Education level ($\beta = -.012$, $p = .895$), leadership role ($\beta = .141$, $p = .122$), experience at the current position ($\beta = -.081$, $p = .292$), and primary cloud computing strategy ($\beta = -.060$, $p = .458$) were not significant predictors. However, experience in cloud computing ($\beta = -.230$, $p = .003$) and industry type ($\beta = .442$, $p < .001$) were significant predictors. The findings suggest that IT leaders' PeS and PeP, along with greater industry maturity and cloud experience, contribute to stronger intent to adopt ML security models. The implications for positive social change include the potential for organizational leaders and IT trainers to implement targeted PeS and PeP awareness programs that improve responsible data handling and cloud security practices, benefiting employees, organizations, and the public through enhanced data protection and reduced risks of security breaches.

The Impact of Machine Learning Security Models on Cloud Data Security

by

Ali Sanad

MS, Walden University, 2022

BS, Colorado State University, 2019

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

October 2025

Dedication

I dedicate this project to God Almighty, my mother, and my wife, who have supported me, believed in me, and encouraged me throughout this long journey. My mother accompanied me with the utmost care, love, and passion. My wife unconditionally encouraged me to pursue my dream and finish my DIT study.

Acknowledgments

Words cannot express my gratitude to Dr. Nawaz Khan chair of my committee. I am thankful for his dedication, patience, and guidance in providing me with feedback to ensure my success. I couldn't have gone this far without the respected committee members and program director, who provided me with generous knowledge and expertise.

I am also truly thankful to my professors, classmates, and cohort members for their moral, emotional, educational, and literal support, and to the writing center and library team members who have truly impacted my progress in this study. Finally, I would like to dedicate a special acknowledgment to my wife, to whom I'll be in debt, for taking on several parental roles to ensure I had the time and the circumstances needed to complete this journey.

Table of Contents

List of Tables	v
Section 1: Foundation of the Study.....	1
Background of the Problem	1
Problem Statement and Project Purpose	2
Problem Statement.....	2
Purpose Statement.....	2
Nature of the Study	3
Research Question	6
Hypotheses.....	6
Theoretical Framework.....	7
Definition of Terms.....	8
Assumptions, Limitations, and Delimitations.....	12
Assumptions.....	12
Limitations	12
Delimitations.....	13
Significance of the Study	13
Contribution to IT Practice	13
Implications for Positive Social Change.....	14
A Review of the Professional and Academic Literature.....	14
Strategy for Searching the Literature.....	15
Theoretical Foundation	16

Early Seminal Work.....	16
TAM.....	17
Analysis of TAM Components	19
Studies Contrasting TAM	20
Studies Based on TAM.....	21
Studies Investigating ML for Cloud Security	29
ML Impact on Threat Detection	33
ML Algorithms for Securing Cloud Computing Environments	36
ML Models for Privacy and Security in Cloud Environments	38
Comparing Non-ML Security Techniques Against ML Models	38
Literature Gap	39
Transition and Summary.....	40
Section 2: The Project.....	42
Purpose Statement.....	42
Role of the Researcher	43
Participants.....	44
Research Method and Design	46
Method	46
Research Design.....	47
Population and Sampling	49
Ethical Research.....	52
Instrumentation	55

Data Collection Technique	59
Data Analysis	60
Research Question and Hypotheses	60
Statistical Analysis.....	61
Data Cleaning and Screening.....	65
Testing Assumptions.....	66
Interpreting Inferential Results	67
Statistical Software	68
Study Validity	68
Threats to External Validity.....	68
Threats to Internal Validity	69
Threats to Statistical Conclusion Validity	69
Rationale for Generalizing Findings to a Larger Population	70
Transition and Summary.....	71
Section 3: Application to Professional Practice and Implications for Change	72
Overview of Study	72
Presentation of Findings	73
Descriptive Statistics.....	73
Test of Assumptions	78
Inferential Results	79
Theoretical Discussion of Findings	82
Application to Professional Practice.....	84

Implications for Social Change.....	86
Recommendations for Action	88
Recommendations for Further Research.....	90
Reflections	92
Summary and Conclusion.....	93
References.....	95
Appendix A: G*Power Analysis to Determine Sample Size.....	113
Appendix B: Invitation	114
Appendix C: Aburbeian et al. (2022) Permission to Use.....	115
Appendix D: Instrument Used to Collect Data.....	116

List of Tables

Table 1 Types of Academic Articles Reviewed	15
Table 2 Professional Experience in Cloud Computing.....	74
Table 3 Item 1 Used for DV Calculation	76
Table 4 Item 2 Used for DV Calculation	76
Table 5 Item 3 Used for DV Calculation	76
Table 6 Item 4 Used for DV Calculation	77
Table 7 Item 5 Used for DV Calculation	77
Table 8 Descriptive Summary of HLR.....	80
Table 9 Regression Summary of HLR.....	81

Section 1: Foundation of the Study

Background of the Problem

Cloud environments are becoming the industry standard for user-based applications and services, particularly in high-performance computing. Organizations adopt cloud-computing environments as Software as a Service to provide increased computational efficiency, continuous integration, and continuous delivery. Nevertheless, the exposure to potential threats generates security risks that affect cloud-based applications. For example, data breaches in cloud environments are often the result of misconfiguration and architectural errors (Tella et al., 2020), which tend to arise when anomaly detection protocols are based only on previously known application attacks (Li et al., 2020). Architectural errors expose cloud-based applications to malicious requests, including cross-site scripting, Structured Query Language injection attacks, and other unauthorized requests that affect exposed application programming interface endpoints.

The findings of previous studies have shown that machine learning (ML) security models can significantly improve data security in cloud environments by improving anomaly and threat detection (Nassif et al., 2021). Because the implementation of ML security models depends on the decisions of information technology (IT) leaders and project managers, the purpose of this study was to examine the relationship between IT leaders' comprehension regarding the perceived security (PeS) and perceived privacy (PeP) of IT professionals with the intent to adopt ML security models in cloud environments.

Problem Statement and Project Purpose

Problem Statement

The rise in demand for cloud-based applications has increased the need for smarter and more robust solutions for solving security problems (Nadeem & Lee, 2020). Shyam and Doddi (2019) suggested that security solutions based on ML and artificial intelligence can reduce data security risks within cloud infrastructure by 18%, compared to non-ML solutions. However, a potential problem that can limit the implementation of ML models in the IT industry is the PeS and PeP of IT professionals regarding ML security models, as shown in the studies of Shyam and Doddi (2019) and Tella et al. (2020). The general IT problem of the current study was that many IT leaders fail to adopt ML models. The specific IT problem was that some IT leaders lack comprehension regarding IT project managers' PeS and PeP and the impact of these factors on the intent to adopt ML models for securing data in cloud-based applications. Additional (control) independent variables were considered to account for other factors that can affect the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type.

Purpose Statement

The purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications after controlling for the respondents' education level, leadership roles, experience at the

current position, experience in cloud computing, primary cloud computing strategy, and industry type. The independent variables were PeS and PeP. The dependent variable was the adoption of ML models in cloud environments for securing data in cloud-based applications. The target population consisted of IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook. The contribution of this study to potential positive social change is the identification of perceptions that are relevant in promoting the adoption of ML security models. The adoption of ML security models may enhance security and privacy in cloud environments, reducing the risk of threats and attacks. This positive social contribution is particularly relevant for the protection of sensitive personally identifiable information (PII), which if stolen from the cloud due to a security breach, can be used maliciously.

Nature of the Study

The nature of a study refers to the research method (i.e., quantitative, qualitative, or mixed methods) and the research design (e.g., a correlational design). In this study, a quantitative method was used to examine and measure the relationship between the dependent variable (adoption of ML models) and the independent variables (PeS and PeP). Additional (control) independent variables were included to account for other factors that can affect the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. The quantitative method used in this study included the application of

hierarchical linear regression (HLR) analysis. Quantitative methods, which involve the analysis of numerical data and statistics, were employed to examine and analyze observable topics (see Aburbeian et al., 2022). Although qualitative research can provide insights into worldview experiences, it was not used in the current study because the focus was on the relationship between PeS and PeP and the adoption of ML models in cloud environments. Mixed methods, which combine quantitative and qualitative results (Li et al., 2020), were not applied because the qualitative component was not implemented in the current study. Quantitative methods based on multiple regression were selected because the purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications.

The quantitative correlational design was chosen due to the categorical nature of the dependent and independent variables. Other methods, such as *t* tests and traditional linear regression based on ordinary least squares (OLS), would not have been appropriate because both the dependent and independent variables were categorical, and one of the key assumptions in other methods is that the variable of interest is not categorical but rather continuous and with a normal distribution. In a hierarchical generalized multiple linear regression model, the dependent variable does not need to have a normal distribution, and optimal estimators can be obtained with maximum likelihood (Agresti & Coull, 1998). Generalized linear models have been validated in applied sciences by Pardo (2020), and have been used to analyze people's perceptions of technology in studies

conducted by Isautier et al. (2020) and Narayana et al. (2020). Previous studies, such as those of Rabe and Kostka (2024), Nambiar and Bolar (2023), and Chauhan et al. (2021), applied a transformation of the variables to accommodate an MLR in the empirical application of the technology acceptance model (TAM).

Designs within quantitative methods can be classified into four categories: correlational, quasi-experimental, experimental, and descriptive. In the current study, a correlational design was used to assess and measure the relationship between variables. In contrast, quasi-experimental and experimental designs establish causal relationships between variables, with the latter allowing for randomization in examining potential causation (Bloomfield & Fisher, 2019). Quasi-experimental and experimental designs were not appropriate for the current study because no experiments were conducted. A descriptive design focuses on the observational aspect of studies (Frazer et al., 2022) and therefore cannot be used to establish relationships among the variables in question. According to Frazer et al. (2022), the descriptive quantitative design includes various types of studies such as case studies, case series, cross-sectional studies, prospective studies, and case-control studies. In the current study, a descriptive design was not employed because the purpose of the study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications.

A correlational design was selected because the research question and hypotheses addressed the relationship between the independent variables and the dependent variable. Other designs, based on causal effects, would not have been appropriate because non-

experimental or quasi-experimental methods were not applicable in the study. The correlation in the study was estimated through an HLR applied to the collected data. To obtain this correlation, the categorical answers of the IT professionals were dichotomized into two categories related to the adoption of ML security models in environments. This transformation into dichotomous variables was applied in studies such as those of Rabe and Kostka (2024), Nambiar and Bolar (2023), and Chauhan et al. (2021), who applied a transformation of variables to accommodate an MLR in the empirical application of the TAM.

Research Question

Is there a relationship between IT leaders' comprehension regarding project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications, after controlling for the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type?

Hypotheses

The null hypothesis (H_0) of the study posited that there is no statistically significant relationship between IT leaders' comprehension regarding project managers' PeS and PeP with their intent to implement ML security models for securing data in cloud-based applications, after controlling for the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. The alternative hypothesis (H_1) posited that there is a statistically significant relationship between IT leaders'

comprehension regarding project managers' PeS and PeP with their intent to implement ML security models for securing data in cloud-based applications, after controlling for respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. As suggested in H_1 , IT leaders' comprehension of project managers' PeS and PeP may significantly influence their decisions to implement ML security models. The comprehension of these factors may play a vital role in determining their adoption of ML-based security solutions for securing their cloud-based applications' data.

The control variables included in the omnibus regression model were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. From this set of control variables, only experience in cloud computing ($\beta = -.230$, $p = .003$), and industry type ($\beta = .442$, $p = .000$) were significant.

Theoretical Framework

The theoretical framework of this study was the TAM, proposed by Davis (1989). The TAM addresses the adoption of new technology among users and highlights the design problems of the information system before its use becomes prevalent (Kamal et al., 2020). The TAM was created to remedy the lack of valid measures available for forecasting and predicting user acceptance of new technologies. Davis identified the most influential variables that affect users' intentions to use new technology, such as perceived usefulness (PU) and perceived ease of use (PEOU). *PU* is defined as the degree to which

a person believes that using a particular system would enhance job performance, and *PEOU* refers to the degree to which a person believes that using a particular system would be effortless (Sagnier et al., 2020).

Definition of Terms

C4.5: A decision tree algorithm that exploits information gain rate as the basis to split attributes. When the continuous attributes are discretized, the algorithm calculates the information gain rate of all the segmentation points (Wang & Gao, 2021).

Clustering-based local outlier factor: An extension of the local outlier factor that combines the concepts of local density and clustering to identify outliers (Ersoy, 2021).

Half-space tree: A machine learning algorithm that detects anomalies in high-dimensional data by recursively partitioning the data using half-spaces (Huang & Li, 2022).

Infrastructure as a Service: The cloud computing model in which a third-party provider hosts and manages the infrastructure required to run applications, such as servers, storage, and networking components (Ramesh et al., 2022).

Isolation forest: An unsupervised ML algorithm that identifies anomalies by isolating outliers in the data (Liu et al., 2021).

Keystroke-level model: An approach to human-computer interaction that is applied for profiling data sets to prevent security attacks for cloud computing (Disha & Waheed, 2022).

Lightweight on-line detector of anomalies: A projection-based detector that constructs an ensemble of one-dimensional histogram density estimators using sparse random projections (Ntroumpogiannis et al., 2023).

Local outlier factor: An ML algorithm used to detect anomalies in data by measuring the local density deviation of a data point concerning its neighbors (Alghushairy et al., 2020).

Locally selective combination: An ML algorithm used for detecting anomalies in high-dimensional data. Locally selective combination works by recursively partitioning the data using half-spaces (Moso et al., 2021).

Locally selective combination in parallel outlier ensembles: A fully unsupervised framework that allows for combining detectors selectively by emphasizing data locality (Butt et al., 2020).

ML algorithm: Computational methods designed to enable machines, typically computers, to learn patterns or make predictions from data through the implementation of statistical techniques. The four types of ML algorithms are supervised, unsupervised, semisupervised, and reinforcement (Jha & Sharma, 2021).

ML models: The output and/or final product of ML algorithms produced after being trained from a data set. The types of ML models include supervised, unsupervised, reinforcement, classification, regression, clustering, dimensionality reduction, and deep learning (Nassif et al., 2021).

ML techniques: The techniques applied to formulate, estimate, and implement ML security models for tackling security issues, threats, and/or attacks within a specific environment or infrastructure (Shyam & Doddi, 2019).

Michigan State University Intrusion Detection Systems Laboratory Knowledge Discovery and Data Mining (KDD) Data Set: A data set used for conducting experiments related to network security (Dutt, 2021).

NSL-KDD: A network-based intrusion detection system data set suggested to solve some of the inherited problems of its parent KDD'99 data sets to help determine the security of systems and alarms for intrusion (Chkirbene, Abdallah, et al., 2021; Chkirbene, Hamila, et al., 2021).

One-class support vector machine: An ML algorithm used to identify and profile user activities (Disha & Waheed, 2022).

Platform as a service: A defined cloud computing model in which a third-party provider hosts and manages the infrastructure and tools required to develop, test, and deploy applications (Yussupov et al., 2021).

Random classification algorithm for rare events: An ML model used to measure the accuracy, sensitivity, and specificity of the proposed KLM-PPSA scheme (Elmrabit et al., 2020).

Regularized class association rules: A model that allows the production of rules-based classifiers in a categorical data space, thereby allowing the building of classifiers that are as accurate as the state algorithms (Mesfer Alshahrani et al., 2022).

Robust random cut forest: An algorithm that first randomly selects a subset of features (dimensions) from the input data and then constructs a binary tree by recursively partitioning the data space along the selected dimensions. At each step, a random feature and a random split point along that feature are chosen. The anomaly score for a data point is calculated based on the average isolation depth across all trees in the forest (Pang et al., 2023).

Semisupervised learning algorithms: A hybrid of supervised and unsupervised learning algorithms in which a smaller portion of labeled data and a larger portion of unlabeled data are used to produce the models (Sana et al., 2021).

Software as a service: A cloud computing model in which a third-party provider hosts and manages software applications and provides them to customers over the internet (Rahman & Pribadi Subriadi, 2022).

Supervised learning algorithm: An ML technique that applies labels within data sets. This technique is often used to train models with well-defined and known data sets; therefore, the input and output have labels. The labeled approach can provide higher accuracy measures over a shorter period when compared to unsupervised learning algorithms (Ismail & Islam, 2020).

Software development life cycle: The methodology used by software developers to design, develop, and maintain high-quality software products (Navaei & Tabrizi, 2022).

Unsupervised learning algorithm: An ML technique that learns through the analysis and clustering of unlabeled data sets. This technique allows for discovering

hidden patterns in the data, thereby allowing the models to be more accurate in further predictions (Tripathy et al., 2020).

UNSW-NB: A network intrusion data set of 175,341 records and 82,332 records of test data that contain nine different attacks including DoS, DDoS, Backdoor, Fuzzers, and other network-based attacks in addition to raw network packets (Chkirbene et al., 2021).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are conjectures, anticipations, assertions, or doctrines postulated by researchers that necessitate evaluation or scrutiny (Mayayise, 2021). The main assumption made in the current study was that IT leaders and project managers influence the adoption of ML security models in cloud-based environments for safeguarding information. The data collection methods were used with the assumption that IT professionals answering the survey would provide accurate and truthful responses and that the outcomes obtained would apply to their corresponding population groups.

Limitations

Limitations are restrictions and constraints that affect the output of a study (Webb & Aly, 2020). The major limitation of the current study lay in the data acquisition because the non-probabilistic data collection of the research design limited the generalizability of the results beyond the analyzed population group. Further, malicious attack simulations can be difficult to measure and compare to real-world scenarios due to the rapid change in cloud security (Nassif et al., 2021).

Delimitations

Delimitations refer to the scope of a study, specifically the characteristics that arise from the limitations coming from the boundaries of what is included and what is excluded in a study (Coker, 2022). In terms of delimitations, this study was confined to the bounds of ML security models and cloud infrastructure. Additionally, the scope of this study was limited to investigating the relationship between the perceptions of IT professionals with the adoption of ML security models. The answers of IT professionals with less than three years of experience were excluded from the study, but the answers of more experienced IT professionals (with three or more years of experience) were included. Additionally, small- to medium-size organizations were excluded from the study because the solutions for those businesses are typically managed by third-party providers. In this study, only the information of IT professionals working in companies with 100 or more employees was analyzed.

Significance of the Study

Contribution to IT Practice

ML is widely known for its capacity to improve accuracy in predictions of target variables of interest, such as the presence of anomalies in data, but the implementation of ML technology generates concerns regarding potential data security and data privacy issues (Tella et al., 2020). The contribution of the current study to the IT practice is the identification of perceived data security and data privacy factors that can influence the adoption of ML models for securing information within cloud infrastructures. This is beneficial because ML security models automate the evaluation of security

implementations within the software development life cycle (Tella et al., 2020) and provide a real-time threat detection system that identifies and filters threats when conducting vulnerability scans and/or data processing (Alsharif & Rawat, 2021). The survey results gathered by Nassif et al. (2021) indicated that ML models provide major benefits in addressing specific data security, data privacy, and trust management issues for cloud infrastructure, particularly in the case of stochastic vector machines.

Implications for Positive Social Change

According to Varghese and Jose (2021), ML security models can increase the security of applications in cloud infrastructures. ML security models can affect social change in organizational environments by improving the security of providers' and consumers' data (Alsharif & Rawat, 2021). Using ML security models within cloud infrastructures can help protect PII and other data for users across the world in multiple industries (Tripathy et al., 2020), which may improve the attitudes of users toward technology and reduce concern about data exposure.

A Review of the Professional and Academic Literature

A comprehensive review of the relevant scholarly literature was conducted to evaluate the recent status of knowledge and techniques associated with data security and data privacy in cloud environments. The critical analysis and study of the literature review was structured into five key areas: (a) theoretical framework, (b) the application of ML for identifying threats, (c) ML models for security in cloud computing, (d) ML data security strategies, and (e) a comparison of ML and non-ML security techniques.

Strategy for Searching the Literature

The strategy used for searching the literature was to divide the search into three types of keywords: (a) keywords specific to ML security strategies within a cloud infrastructure; (b) keywords related to IT managers and leaders, their perceived security and privacy, and their intention to implement security tools within a cloud infrastructure; and (c) keywords specific to articles that use TAM or any other modern extensions of this theory as a theoretical framework. The specific keywords used were *ML security models*, *ML security strategies*, *ML for securing cloud infrastructure or cloud data*, *cloud infrastructure security techniques*, *IT managers*, *perceived security* or *perceived privacy within a cloud infrastructure*, *ML security model for cloud applications*, *TAM for accepting ML strategies for security*, and *IT managers implementation of ML security strategies or techniques*. The Walden University Library databases that were used for searching relevant literature were EBSCO, ProQuest, Science Direct, Academic Search Complete, and Google Scholar. The comprehensive categorized literature collected 109 articles, as shown in Table 1.

Table 1

Types of Academic Articles Reviewed

Article type	Number of articles	Percentage
Peer reviewed	100	92%
Seminal work	9	8%
Total	109	100%

Theoretical Foundation

The theoretical foundation of this study was the TAM. The supporting theories of TAM are the theory of reasoned action (Ajzen & Fishbein, 1975) and the theory of planned behavior, according to Al-Emran and Granić (2021). Contrasting theories to the TAM include the hedonic-motivation system adoption model, which is a theoretical framework for describing the adoption of inherent or hedonic frameworks. In the case of technology adoption, the choice of an individual to accept new technology is known as technology acceptance (Kamal et al., 2020). Several frameworks have been developed to explain the factors that affect technology acceptance, such as the TAM, the theory of planned behavior, the diffusion of innovation theory, the theory of reasoned action, the motivational model, the unified theory of acceptance, and the social cognitive theory (Nyimbili & Chalwe, 2023). These theories are based on cognitive components, specifically attitudes, social norms, intentions (in the case of the theory of reasoned action), perceived behavioral control of resources (in the theory of planned behavior), opportunities, skills, habits, and facilitating conditions (in the theory of interpersonal behavior).

Early Seminal Work

The TAM was developed by Davis (1989) as an extension of the theory of reasoned action, which was proposed by Ajzen and Fishbein (1975) as a mathematical model to help researchers predict behavioral intentions as a function of subjective norms and attitudes. Ajzen and Fishbein implemented the model as an improvement of the information integration theory by introducing three major components: beliefs,

intentions, and attitudes. The theory of reasoned action was designed to aid in understanding the relationship between these components, and it is rooted in the idea that intentions are the main predictors of behavior, which allows for a way to measure an individual's intention of adopting a technology (Ajzen & Fishbein, 1975). Researchers interested in investigating the adoption of new technology began implementing the theory to examine users' behavior toward the newly introduced technology based on intentions, beliefs, and behavior (Ajzen & Fishbein, 1975). Ajzen and Fishbein identified intention as the readiness to perform a given task, belief as the chance of an object or entity to provide or acquire attributes, and attitude as the evaluation of that object.

TAM

Al-Emran and Granić (2021) noted that the TAM is a powerful and parsimonious model that can be applied as a theoretical framework to represent system use based on the perceptions of users because perceptions influence attitude toward use, which determines behavioral intention. Through perceived factors, the TAM provides a method of identifying the motivations behind the adoption of new technologies. Additionally, the TAM helps to explain the motivation behind IT decisions (Musyaffi & Arinal, 2021), with PU and PEOU being the two main factors influencing users' decisions in the TAM (Mayayise, 2021). Mariani et al. (2021) noted that the TAM has dominated the social science field as the main model for adopting and accepting new technologies and information systems. Similarly, the results of a survey conducted by Lah et al. (2020) showed that the TAM and its modified version, mTAM, can help researchers identify predictors of users' decision making when adopting new technologies. The TAM seeks to

anticipate the adoption of new technology among users and to highlight the design problems of the information system before its use becomes prevalent among people (Kamal et al., 2020). In the TAM, the motivation of users is influenced by three factors: PU, PEOU, and attitude toward use (Nyimbili & Chalwe, 2023). Sagnier et al. (2020) noted that the TAM is based on two psychosocial theories seeking to explain and predict a specified behavior: the theory of reasoned action and the theory of planned behavior.

The TAM was created to remedy the lack of valid measures available for forecasting and predicting the user acceptance of new technologies. Davis (1989) identified the most influential variables affecting users' intentions of using new technology, including PU and PEOU. PU is defined as the degree to which a person believes that using a particular system would enhance job performance, and *PEOU* refers to the degree to which a person believes that using a particular system would be effortless (Sagnier et al., 2020). In their review of technology acceptance and adoption models and theories, Nyimbili and Chalwe (2023) found that PU affects the adoption of new technologies due to its correlation with perceived self-reported current use and self-predicted potential use. To account for external variables affecting the decision to adopt new technology, researchers have proposed extensions of the TAM by considering concepts such as performance expectancy, social influence, effort expectation, and facilitating conditions (Rafique et al., 2020). Based on the original TAM and the extensions proposed to include additional control covariates, previous studies have been conducted to identify the factors affecting the adoption of new technologies. For example, Alfadda and Mahdi (2021) used the TAM to gain insights into the correlation of

user reactions to the technology adopted for language learning, and Vahdat et al. (2021) used the TAM as a framework to examine social influence and peer influence in the adoption of app technologies. In the case of Vahdat et al., PU was not found to have a significant effect on attitude toward app use, but PEOU and external factors contextual to the study, such as social and peer influence and intention to purchase, had positive effects on technology adoption.

Analysis of TAM Components

According to Davis (1989), the components of the TAM are (a) PU, (b) PEOU, (c) behavioral intention to use, and (d) actual system use. These components help to understand how a user will likely react toward a new technology before seeing or interacting with it. Understanding the components of the TAM and how they are used in technology acceptance is critical within computer information systems.

The components of the TAM also provide the means for assessing the effects of system attributes on users (Davis, 1989). Al-Madhagy Taufiq-Hail et al. (2021) noted that the TAM is one of the most extensive and in-depth tools for understanding the adoption of technology by users. The TAM's components and structure make it a powerful and effective theoretical framework for exploring how users will adopt a given technology based on PU and PEOU, where PU is defined as how users predict a technology will affect them in their everyday lives, and PEOU is defined as the amount of training expected to be needed to get started with the technology (Hatmawan & Taufiq, 2021). Ferri et al. (2020) also showed that individuals' perceptions of how easy a given technology is to use act as a base for their cognitive behavior on their desirability within

PU. If the technology presented to users does not appeal to their PEOU, the adoption of the technology or product will be limited.

Li et al. (2020) also indicated that understanding PEOU can increase productivity and efficiency within a work environment. Similarly, Musyaffi and Arinal (2021) noted that PU can impact CEOs' technological decision making for their teams' work environments. Such observations can affect attitudes toward technologies, especially when incentives involve performance in work environments. Davis (1989) illustrated how TAM components work together by starting with external variables and factoring in PU and PEOU, which results in creating attitudes toward using technologies, which leads to behavior intention to use and actual system use.

Over the past three decades, researchers have used the TAM in multiple technological studies to understand factors influencing users' acceptance of technologies. PU and PEOU are the two major components of TAM that aid in understanding why certain technologies are used. The components of the TAM were appropriate for examining and analyzing the components of the current study because the TAM had been applied to evaluate user acceptance and adoption of new technologies (see Sagnier et al., 2020).

Studies Contrasting TAM

Al-Emran and Granić (2021) noted that the TAM is not appropriate for use in all applications because it excludes constructs such as perceived risk. Opposing theories have emerged to complement or extend the TAM. Al-Emran and Granić indicated that the TAM is not relevant for describing the adoption of inherent or hedonic frameworks

(e.g., learning for pleasure or music), and in this case the hedonic-motivation system adoption model is a better theoretical framework. Malatji et al. (2020) applied a bibliometric analysis to evaluate whether the TAM is a valid or outdated theory. Malatji et al. argued that although most of the research dealing with the TAM focused on finding behavioral intention antecedents; to properly apply the TAM, factors must be included to moderate the relationships among TAM variables. Extended TAM studies applied an expansion of the original TAM by including external variables with an intention to investigate the outcomes of external factors on user attitude to overcome the limitations of the traditional TAM.

Studies Based on TAM

Webb and Aly (2020) applied the TAM and the unified theory of acceptance and use of technology (UTAUT) to evaluate whether security concerns are a factor in accepting virtual private cloud (VPC) when individuals believe that VPC solutions are introduced to solve security issues within a cloud infrastructure. Sagnier et al. (2020) applied the TAM as a theoretical framework to better understand the adoption of virtual technology within organizations. Razali et al. (2021) conducted a TAM-based study extending the technology readiness and acceptance model and showed that security vulnerabilities in government intelligence agencies are located in data-sharing endpoints. Hanif and Lallie (2021) applied the TAM and user acceptance testing and found that performance expectancy, effort expectancy, and social influence are highly correlated to the adoption of security measures for cloud computing. These findings help to deepen the

understanding of the security risks associated with cloud computing and the adoption of technological tools for solving security issues and vulnerabilities in cloud environments.

Other studies proposed conceptual models for the adoption of cloud computing security measures based on TAM to verify and investigate the suitability of the proposed technology. Tissir et al. (2020) implemented the TAM to measure cloud computing acceptance by the Government of Croatia. Their study applied the TAM and technology organization environment framework to assess the actual system used by analyzing PE and PEOU within government auditors and other employees. The findings showed that PeS, PE, and PEOU are the major factors of cloud technology acceptance. These findings align with those of Hanif and Lallie (2021) in that cloud infrastructure security is no longer a key concern for IT managers and leaders, but rather the configuration and architectural errors that cause security vulnerabilities. Al-Madhagy Taufiq-Hail et al. (2021) evaluated the factors influencing SaaS implementation within cloud infrastructures. Their study applied the TAM to evaluate PU and PEOU jointly with the theory of planned behavior. The findings were similar to those of Razali et al. (2021), suggesting that cloud infrastructure security is not a determinant of SaaS adoption. Rather, PU, PEOU, and the subjective social norms of IT professionals were the dominant factors in predicting SaaS adoption (Al-Madhagy Taufiq-Hail et al., 2021). These results indicate that security concerns affecting the infrastructure do not significantly impact the decisions of IT professionals; instead, PEOU and PU are the dominant factors affecting the adoption of new technology.

Changchit and Chuchuen (2018) also discussed the factors affecting the adoption of cloud computing services, framed on the TAM, in the context of training and education, complexity, compatibility, and organizational readiness to measure cloud computing adoption. Changchit and Chuchuen found that infrastructure security was not a significant factor in technology adoption. Instead, the most significant factor in cloud computing adoption was PEOU because CEOs and project managers did not want to be tied to a particular set of technologies or to provide training for employees to use the new systems. Similarly, Ferri et al. (2020) conducted a study on small- to medium-size enterprises in Italy that assessed how risk perception influences technology adoption by the CEOs of the enterprises. Ferri et al. used the TAM as a theoretical framework to investigate and predict system use and attitudes toward the technology. Ferri et al. implemented a structural equation modeling approach using a survey based on the Likert scale, and they concluded that PU had the strongest positive effect on technology implementation intention, while perceived cloud security did not significantly impact technology adoption.

Musyaffi and Arinal (2021) also used the TAM to investigate the factors for cloud adoption within accounting enterprises and small accounting firms. Musyaffi and Arinal concluded that PU and PEOU were the two major factors affecting the acceptance of cloud technology, with the security concerns relating mainly to the specific data storage, sharing, and manipulation of services residing on the cloud. Musyaffi and Arinal applied Cronbach's alpha and average variance extracted to evaluate the validity of their findings. Their study was conducted with 123 accounting students within six different classes

enrolled in a business college. Musyaffi and Arinal (2021) used an online survey to ask students about their 6 months of participation in cloud accounting.

Mariani et al. (2021) created a theoretical model to test an extension of the TAM aimed at analyzing the influence of perceived privacy risks and user trust on digital personal data stores. Mariani et al. based their analysis of these factors on the previous use of digital personal data stores. Their study was conducted using a survey that captured perceived privacy risk, perceived security risk, user experience of digital personal data stores, PU, and PEOU. The survey was conducted online amongst residents in the UK, sampling 214 participants aged 16 to 65. The findings of Mariani et al. (2021) revealed that PEOU was critical in influencing user attitudes toward technology adoption.

Another study, conducted by Stieninger et al. (2022), used an online survey to evaluate and understand the factors affecting the adoption of cloud computing. The study was framed on the TAM and was intended to analyze attitudes toward technology and actual system usage. Stieninger et al. (2022) examined perceived relative advantage, higher level of complexity, better image, higher level of security and trust, and attitude towards cloud adoption. The study revealed that lower levels of complex variables, such as compatibility, security, and trust, lead to a more positive attitude towards the adoption of new technologies. Pankowska et al. (2020) also used the TAM to investigate the factors influencing the adoption of sustainable cloud computing solutions. They concluded that the major and best predictors for actual system use were PU and system and service quality. Hafiz et al. (2022) obtained similar findings after conducting a literature review to investigate technology adoption theories for novelty in building

information modeling. Hafiz et al. specifically aimed to uncover adoption factors for building information modeling. Hafiz et al. found that the major factors influencing the adoption of building information modeling were social influence, subjective norms, and PEOU.

Scholars and experts have noticed hesitance in adopting cloud computing and have begun investigating the factors influencing technology adoption. Aldahwan and Ramzan (2022), for example, conducted a study aimed at investigating the relationship between cloud users' experiences and their adoption of cloud computing in Saudi education institutions. Similar to Stieninger et al. (2022), Aldahwan and Ramzan (2022) designed a survey to collect the answers of 106 individuals within education systems and institutions in the region. Aldahwan and Ramzan found that security concerns significantly influenced the adoption of cloud computing. Their research showed that participants had data security and data privacy concerns regarding cloud infrastructure providers.

Weng et al. (2021) also reviewed technology acceptance models in their study and found that TAM and UTAUT were the two most efficient, accurate, and popular frameworks, arguing that these approaches are the most common in the field of information management. Weng et al. divided the TAM into four aspects: (a) PU, (b) PEOU, (c) attitude toward using, and (d) intention to use. They then conducted a survey using a 5-point Likert scale, ranging from *strongly agree* to *strongly disagree*, based on a convenience sample.

Other researchers have evaluated cloud infrastructure components and architectures in search of privacy and security factors that may impact attitudes toward cloud computing. Webb and Aly (2020), for example, discussed the security concerns within VPC by examining the relationship between users' acceptance and adoption of VPC technologies. Webb and Aly used the TAM and the UTAUT as theoretical frameworks for their study and designed an online survey sampling over 400 qualified IT professionals aged 18 to 65 years in the United States. The survey was aimed to capture participants' PU, PEOU, PeS, perceived trust (PT), and attitude towards usage. The study revealed that PeS and PT had no significant impact on VPC adoption, attitude toward technology, or actual system use (Webb & Aly, 2020).

In a study conducted on the banking industry, Hanif and Lallie (2021) applied UTAUT to investigate the adoption of mobile banking technology. Hanif and Lallie (2021) examined the cybersecurity factors influencing the intention to use mobile banking applications amongst people aged 55+ in the UK, with the aim of measuring which factors influence the intention to use. Hanif and Lallie found that perceived cybersecurity and trust did not significantly impact user adoption. Ismail and Islam (2020) proposed a security audit framework to ensure consistent monitoring of data migration tasks, focusing on security transparency and utilizing the TAM to evaluate technology adoption. These studies both indicated that the factors influencing cloud infrastructure adoption are complex and multidimensional. While security and privacy are important factors to consider, other factors, such as ease of use, quality of service, and

peer influence, can also play a significant role. Researchers should continue to examine these factors and their relative importance in cloud infrastructure.

Other researchers have found that security and privacy issues are a relevant concern in cloud computing implementations. Abdelrahman et al. (2021) analyzed software-defined networking (SDN) and classified SDN controllers into two categories: (a) open source and (b) closed source. Abdelrahman et al. argued that certain security threats can cripple an entire network, including distributed denial of service (DDoS) threats, build-and-run-time-injected malware, insider (tenant) attacks, and security holes resulting from controller misconfigurations. Nassif et al. (2021) found that privacy is one of the most relevant concerns influencing the adoption of ML techniques for improving the security of cloud computing environments.

Al Hadwer et al. (2021) also systematically analyzed factors impacting cloud infrastructure adoption. Their study was framed on the applied technology organization environment theory, originally developed by Tornatzky et al. (1990) to provide a technology acceptance context at the firm level. In their study, Al Hadwer et al. concluded that security concerns were the second-most frequent variable within the technical dimension of the analysis, after top management and support. In a similar study, Sadoughi et al. (2020) investigated the adoption of cloud computing in the healthcare industry. Their study included 47 articles categorized according to the type of industry. Sadoughi et al. found that the major theories affecting the adoption of new technologies are the theory of reasoned action, TAM, diffusion of innovation, technology organization environment, and UTAUT. Sadoughi et al. (2020) argue that security concerns are the

most important factor for healthcare providers, followed by trust and health managers' PU.

Sana et al. (2021) conducted an analysis of PeS dimensions based on POU and PU, with the aim of evaluating the relationship between PeS and the adoption of new technologies in business-to-consumer e-commerce websites in Indonesia. The study of Sana et al. (2021), framed on TAM, showed that PeS is one of the top four factors influencing technology adoption and actual system use in all types of businesses. Sana et al. (2021) concluded that in addition to PeS, the major factors influencing technology adoption in business-to-consumer e-commerce websites are data confidentiality, data integrity, and data availability.

Siagian et al. (2022) also conducted a study framed on the TAM to investigate consumer behavior and digital payments in social media. The study was based on PEOU, PeS, PU, and PT. Siagian et al. used an online survey to collect information from 250 consumers on social media platforms, applying structural equation modeling to conduct the data analysis. The results of Siagian et al. (2022) indicated that PEOU and PT indirectly affect consumer behavior, with PeS being the most significant factor.

Previous studies have used quantitative methods similar to the ones applied in this study, framed on the TAM. Chauhan et al. used regression models with categorical variables to analyze the factors that encourage the expansion of the mobile games industry. Chauhan et al. argued that a high PEOU implies that it is easy to start playing online games as well as to understand the rules of the games. Chauhan et al. (2021) used a 7-point Likert scale survey to collect the answers of 450 participants who play online

games, most of them residing in three cities in Central India (Agra, Gwalior, and Indore). The results of Chauhan et al. (2021) indicated that PU, attitude, and symmetric flow are important factors influencing the adoption of technology in the game industry. Rabe and Kostka (2024) administered an online opinion survey based on a Likert scale to sample participants in Thailand, Indonesia, Malaysia, and the Philippines. After using a generalized linear model based on transformed categorical variables, Rabe and Kostka found that citizens in these countries exhibit higher acceptance rates of social credit systems, with acceptance rates declining significantly if the technologies supporting these systems originated from China. Rabe and Kostka (2024) explained their results by introducing an external TAM based on citizens' attitudes toward their domestic situations and their perceptions of China's potential benefits to their countries. Nambiar and Bolar (2023) examined the factors that affect the preference of cash over banking cards, through a cross-sectional survey based on a 5-point Likert scale. The survey was administered to 521 bank customers from one of the largest banks in India, based on a convenience sampling technique similar to the one used in the current study. The responses were analyzed using generalized MLR and ML models. The results of Nambiar and Bolar (2023) indicated that customers prefer cash over banking cards because of its usefulness rather than customer trust or perceptions of security.

Studies Investigating ML for Cloud Security

Skafi et al. (2020) investigated the adoption of security tools in cloud computing services and found that technological (i.e., complexity and security) and organizational (i.e., top management support and prior IT experience) factors have a positive correlation

with the decision to adopt cloud computing services. The analysis of Skafi et al. also showed that context-specific factors (e.g., poor infrastructure and lack of government initiatives) have a negative correlation with adoption decisions. Through their findings, Skafi et al. suggested that there are security and privacy concerns around cloud infrastructure configuration and the design and architecture that can affect SaaS applications (Tella et al., 2020). Consequently, researchers have begun investigating and exploring security options that can help improve PeS and PeP and attempting to automate the process using ML security techniques.

Several researchers have conducted systematic reviews of the ML models available for securing application data in cloud environments. Nassif et al. (2021), for example, performed a systematic literature review of the methodologies and techniques for securing cloud infrastructures using ML. Nassif et al. (2021) analyzed 63 studies grouped into three main categories: (a) threat types for cloud environments, (b) ML techniques implemented to deter threats, and (c) the performance of each implemented ML model. Nassif et al. (2021) found that the major security concerns within cloud infrastructures were anomaly detection, attack detection, vulnerability detection, intrusion detection, privacy preservation, data confidentiality, data privacy, and DDoS prevention. Nassif et al. also found that over 30 types of ML models have been used as hybrid and standalone tools in cloud environments. The analysis of Nassif et al. showed that ML models had better results as a hybrid security tool when used in any of the 11 security areas identified.

Abdelrahman et al. (2021) analyzed security and vulnerabilities within cloud environments in the context of software-defined networking (SDN), because SDN addresses major cloud computing issues and complements cloud services in terms of network virtualization and networking as a service (NaaS). Abdelrahman et al. found that SDN faces security challenges relating to DDoS threats, injected malware, insider (tenant) attacks, and security gaps from controller misconfigurations. Chkirbene et al. (2021a) discussed the limitations of traditional security tools for cloud environments and proposed an ML model-based firewall called the secure packet classifier (SPC) to enable anomaly detection and classification. Chkirbene et al. (2021a) used a stepwise comparison to show the superiority of SPC over traditional firewalls. Additionally, Chkirbene et al. (2021b) tested SPC with a series of data sets and showed that the SPC achieves 81% accuracy in anomaly detection, compared to an average of 60.5% accuracy obtained with traditional firewalls. Similarly, Butt et al. (2020) highlighted the benefits of ML models in securing cloud computing applications. Butt et al. also provided a review of cloud computing service models that identify attacks, and of the environment in which attacks occur.

The studies conducted by Chkirbene et al. (2021a, 2021b) and Butt et al. (2020) both demonstrate the advantages of implementing ML security models in cloud environments. The SPC firewall proposed by Chkirbene et al. (2021a) is a clear example of how ML algorithms can improve anomaly detection and classification. The comparison between SPC and traditional firewalls highlighted the superiority of ML models, which can significantly enhance the security of cloud environments in many

applications. The study conducted by Butt et al. (2020) highlighted the importance of understanding various cloud computing models and identifying potential attack types to effectively secure cloud applications. Like Nassif et al. (2021), Butt et al. (2020) found that the four major attacks targeting cloud computing were network-based, VM-based, storage-based, and application-based attacks. The two studies emphasize the importance of implementing ML models to enhance the security of cloud environments. By providing effective anomaly detection and classification, ML models can significantly reduce the risk of attacks and improve the efficiency and effectiveness of security policies.

Past studies have been conducted to evaluate security issues and concerns within hybrid cloud environments. Nassif et al. (2021) conducted a systematic literature review of ML and cloud security, and they found that DDoS and data privacy were the most common cloud security concerns, with a 16% and 14% level of use respectively. Nassif et al. (2021) found 30 ML techniques, some hybrid and others standalone, being the most frequently applied support vector machines. Similarly, Du (2022) analyzed the relationship between artificial intelligence and data security within a cloud infrastructure. Du proposed a three-step method for analyzing big data security, data mining security, data transmission security, and applications in cloud environments. Du argued that a model based on artificial intelligence can better recognize various types of biologically based data sets, such as data sets used to collect fingerprints and optical information. In the study of Du (2022), PeS and PeP were significantly impacted by the implementation of continuously evolving artificial intelligence security models.

Mohammad and Pradhan (2021) also proposed an ML-assisted cloud computing model for enhancing the security and integrity of big data in cloud infrastructures.

Mohammad and Pradhan (2021) proposed encrypting data within different locations and servers to reduce overhead and latencies. ML models such as the cloud computing model used by Mohammad and Pradhan improved transmission rate by 96.4%, data management by 94.3%, processing time by 35.2%, performance by 95.2%, and accuracy by 91.7%.

Similarly, Lee and Nadim (2020) proposed an ML model to assist in detecting kernel-level rootkits. *Rootkits* are software utilities that allow unauthorized user access to a particular system (Lee & Nadim, 2020). ML models applied to the detection of kernel-level rootkits are intended to monitor and identify changes in hardware registers, control registers, system-entered registers; global and local descriptor registers; system call alteration; and all-task and run-list system utilities.

Mesfer Alshahrani et al. (2022) proposed an ML model to enhance and optimize security and privacy within cloud environments. The ML model proposed by Mesfer Alshahrani et al. is a network-level anomaly and threat detection model that sits on top of existing non-ML-based security. The comparison study conducted by Mesfer Alshahrani et al. indicated that ML models can enhance performance in threat detection outcomes, compared to non-ML-based security tools.

ML Impact on Threat Detection

Although there are several possible applications of ML models, the most frequent implementation of ML security models in cloud environments relates to threat and

intrusion detection (Butt et al., 2020). Varghese and Jose (2021), for example, developed an intrusion detection system (IDS) model that implements ML to protect cloud networks. Their IDS-ML model contains two components: one that handles extraction, and one that performs classification. The IDS-ML model showed superior performance compared to non-ML IDS after training the model using the UNSW-NB15 dataset, as well as better accuracy compared to traditional ML models based on support vector machines or random forests (Varghese & Jose, 2021).

Other ML models used for anomaly detection are centered around the Trust-based Intrusion Detection and Classification System (TIDCS) and the Trust-based Intrusion Detection and Classification System-Accelerated (TIDCS-A). Both ML-based intrusion detection models produce significant results that ensure efficient network-level security and privacy in cloud environments (Chkirbene et al., 2021a). These models remove unnecessary data and introduce new features generated by the proposed algorithm (Mesfer Alshahrani et al., 2022). First, a supervised ML model uses previously retained information to improve trustworthy connectivity between nodes, and then TIDCS and TIDCS-A implement the best selected features to produce an efficient and well-trained model for attack classification (Alsharif & Rawat, 2021).

One of the challenges of training and implementing ML security models is the limited availability of training data (Chinedu et al., 2021). This limitation has promoted a new generation of ML models adapted to secure information in cloud environments. For example, generative adversarial networks improve the efficiency of an ML model, resulting in more accurate detection when only relatively small training datasets are

available (Chkirbene et al., 2021a). A *generative adversarial network* is an ML model that implements two unsupervised neural networks running simultaneously to produce a more accurate prediction, using a zero-sum framework to acquire learning.

Network Intrusion Detection System (UNSW-NB) and Intrusion Detection Datasets (NSL-KDD) are generally used for conducting experiments that evaluate the performance of ML models (Varghese & Jose, 2021). UNSW-NB and NSL-KDD are highly dimensional data sets representing dense, affluent cloud traffic sections. In experimental settings, 1000 new samples of augmented data spawned from the original data were used to train ML models. Such experiments produced admissible and authentic datasets that can be used to enhance the training of ML security models.

Ersoy (2021) proposed several ML models, based on universal data insights, for monitoring user activities and for user profiling in small datasets. Specifically, Ersoy proposed the following ML security models for detecting abnormal user behavior in small datasets: isolation forests, local outlier factors (LOF), cluster-based local outlier factors (CBLOF), lightweight online detectors of anomalies (LODA), robust random cut forests (RRCF), half-space trees, and locally selective combination in parallel outlier ensembles (LSCP). Ersoy (2021) found that LODA, RRCF, and LSCP were the most accurate and efficient models for user profiling, in terms of algorithm speed, dataset size, accuracy, and time. Alghushairy et al. (2020) argue that outlier detection, specifically LOF, has a major impact on cloud-based applications and plays a significant role in detecting abnormal events in static and stream environments. However, the results of Ersoy (2021) need to be verified with larger datasets and longer model training time.

ML Algorithms for Securing Cloud Computing Environments

Researchers and security experts have proposed new ML models that allow system administrators to help protect cloud data against external attacks. Eddermoug et al. (2021) proposed the keystroke-level model (KLM), a model based on three security factors: (a) K, the number of attempts with an incorrect password; (b) L, the number of attempts with a biometric trait; and (c) M, the number of attempts with a correct password but with an invalid keystroke. These KLM factors aim at profiling and preventing security attacks and are therefore known as the KLM-based profiling and preventing security attacks (KLM-PPSA) model. Eddermoug et al. (2021) conducted three experiments to evaluate the performance of the KLM-PPSA model, using variables such as user and attempt ID, authentication methods, internet protocol (IP) addresses, media access control (MAC) addresses, time, place, keystrokes, and biometric attempts.

Similarly, Ntambu and Adeshina (2021) proposed an ML model to detect and identify anomalies related to cloud-based virtual machines. Ntambu and Adeshina applied isolation forests and one-class support vector machines to identify and profile user activities and behavior accurately. They concluded that one-class support vector machines produced a higher success rate in anomaly detection. The proposed ML-based models have the potential to enhance the security of cloud infrastructure against external attacks and unauthorized user access. As cloud-based infrastructure is becoming more widespread, it is necessary to have robust security measures in place to ensure the safety and privacy of data. Therefore, further research and development in this field could lead to the integration of ML models within monitoring-as-a-service architectures.

Other researchers have suggested that implementing ML algorithms can help mitigate cyber threats and thus reinforce security infrastructures by improving threat detection. Disha and Waheed (2022) showed that ML models based on decision trees improve accuracy and precision in threat detection. New methods based on hyperspectral anomaly detection, such as the half-space trees method, have demonstrated increased effectiveness, efficiency, and accuracy in threat detection (Huang & Li, 2022). Jha and Sharma (2021) proposed a framework for detecting malicious behavior in cloud environments and found that random forest models outperform non-ML models in terms of accuracy, sensitivity, and specificity. Kumar et al. (2022) proposed an ML-based distributed IDS to detect DDoS attacks and mitigate security issues and limitations within internet of things (IoT) devices. Kumar et al. found that the ML distributed detection system increased security measures more efficiently compared to non-ML security tools, demonstrating the feasibility and effectiveness of ML models for threat detection.

Researchers have shown that ML can enhance the security of cloud computing applications by detecting suspicious activities and risks. Navaei and Tabrizi (2022) conducted a comprehensive review of ML implementation within the software development life cycle, and they concluded that ML can have a significant impact on software development within cloud infrastructures from a security testing perspective. Furthermore, Staerman et al. (2022) have concluded that anomaly detection methods are becoming more effective and efficient due to a rise in datasets available, rapid improvements for threat detection algorithms, and the continuous growth and support of research on anomaly detection. The potential for using ML models for securing

applications within cloud infrastructure is promising. For example, random forest classifiers outperform non-ML models by achieving a 99.8% accuracy in anomaly detection (Tripathy et al., 2020).

ML Models for Privacy and Security in Cloud Environments

The emergence of new ML models is revolutionizing security and privacy in cloud environments. The studies conducted by Liu et al. (2021) and Tiwari et al. (2022) analyzed the latest trends and solutions to ML privacy issues. Liu et al. categorized the interaction between ML and privacy into private ML, ML-aided privacy protection, and ML-based privacy attack and protection schemas. They found that ML-aided privacy protection is becoming more widely used within various applications. Due to data complexity, Liu et al. (2021) also showed that new privacy metrics are needed to measure ML privacy evaluation.

In contrast, Tiwari et al. (2022) argued that the construction of ML models should aim to increase data security while maintaining data confidentiality and availability. Tiwari et al. (2022) proposed an ML method to identify and filter any denoised image, file, or document. This ML method can be used as a security strategy to help obtain a higher peak signal-to-noise ratio compared to non-ML techniques.

Comparing Non-ML Security Techniques Against ML Models

The current state of data security within organizations mainly relies on non-ML-based techniques, but experiments have been conducted to compare non-ML security techniques against ML models. Sauber et al. (2021) developed an ML model based on private, secret, and public keys, and they used encryption to protect data from fake

authorized identity users. Sauber et al. tested their ML model using the Java-based framework and found that the model effectively protected data from attacks coming from unauthorized and unidentified users. In the study of Sauber et al., their model was found to enhance the security of cloud computing by improving the encryption of data in the cloud and protecting the system from any fake data owner who enters potentially harmful information. Specifically, Sauber et al. (2021) developed a one-time password technique to protect users and data owners from any fake unauthorized access to the cloud.

Chinedu et al. (2021) conducted a literature review of ML implementations for cybercrime detection and prevention. In their study, Chinedu et al. examined 120 articles and found that no model had been successful in helping to fight cybercrime within the last decade, highlighting the need for novel approaches to data security and cybercrime prevention. Chinedu et al. highlighted various categories of cybercrimes, providing a comprehensive review of cybercrime detection and prevention models based on ML and other intelligent systems. Chinedu et al. concluded that the applicability of ML for curtailing or containing cybercrimes in the cyberspace faces setbacks due to the unavailability of adequate cybercrime datasets across various threat and attack domains, limited scope, and limited adaptability and reproducibility in real-world environments.

Literature Gap

Several studies have been conducted to delve into the impact of ML models for improving security and privacy in cloud environments. However, despite the abundance of peer-reviewed articles on this topic, there remains a gap in academic literature regarding the role that IT managers and leaders play in the implementation of ML models

in cloud environments. Particularly, no study has been conducted to evaluate the influence of the PeS and PeP of IT professionals on the adoption of ML models in cloud environments. To fill this gap, the purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications. The independent variables were PeS and PeP. Additional (control) variables were considered, specifically the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. Although some peer-reviewed articles suggested that security within cloud infrastructures is not a significant factor in determining the adoption of ML models (Ismail & Islam, 2020), the majority of the literature reviewed indicated that security and privacy within cloud applications are a major concern for IT managers and project leaders (Siagian et al., 2022).

Transition and Summary

Previous studies have found that ML models can improve security and privacy in cloud environments. However, no study has been conducted to evaluate how the perceptions of IT professionals influence the adoption of ML models in cloud environments. Thus, the purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications. Framed on the theory of the TAM, the research question and hypothesis of

the study address the relationship between IT leaders' comprehension of IT project managers' PeP and PeS with the intent to adopt ML models in cloud environments.

Section 2 will include details about the online survey used to collect the information needed to test the hypothesis and answer the research question of this study. Detailed explanations will be given about the purpose statement, the role of the researcher, the population and sampling strategies, the research methods and design, the ethical framework of the research, the data collection process, and the selected statistical analysis methods.

Section 2: The Project

This section includes details about the purpose statement, the role of the researcher, the population and sampling strategies used for selecting the participants, the research methods and design, the ethical framework of the research, the data collection process, and the methods of statistical analysis applied.

Purpose Statement

The purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications. Additional (control) variables were considered to account for other factors that can affect the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. The independent variables were PeS and PeP. The dependent variable was the adoption of ML models in cloud environments for securing data in cloud-based applications. The target population was IT project managers and leaders with three or more years of experience designing and implementing cloud-based applications in organizations and institutions in South Loop in Chicago, University Park, and Oakbrook. The implications for positive social change include the promotion of the adoption of ML security models that may aid in improving the security and privacy of cloud-based applications and reduce the risk of threats and attacks. This is particularly relevant for the protection of sensitive PII, which can be used maliciously if stolen due to data leaks.

Role of the Researcher

Aburbeian et al. (2022) discussed the importance of the researcher's relationship to the topic when conducting a study because it helps to define the appropriate scope of research, resources available, methodology, participants, and other research components. I had a specific relationship to the topic and area of research due to my position as a technical leader responsible for building and maintaining cloud-based software solutions. In my daily activities, I am involved in the design of data security and data privacy architectures. My responsibilities extend beyond software solutions and include duties relating to network traffic security and other communications channels. Although I had never implemented ML-based models, I had implemented several non-ML-based solutions to enhance security in web applications.

In this quantitative correlational study, I emphasized the implementation of appropriate mathematical and statistical tools suitable for analyzing categorical data. Based on the results and recommendations of Sana et al. (2021) regarding enhanced security in cloud computing, in the conceptualization of the study, I provided an accurate description of the IT problem, a definition of the formulated concepts, a selection of dimensions and indicators implied by the concept, and an identification of how the concept would be measured. The data in this study were collected through an online survey and were used to answer the research question, test the hypotheses of the study, and draw conclusions based on the results. The online survey fit the scope of the research and was administered with the use of web-based tools aligned with the ethical principles and guidelines outlined in the Belmont Report protocol. The National Commission

created this protocol to protect human subjects involved in behavioral research, with the three basic principles being respecting persons, beneficence, and justice (Alghushairy et al., 2020).

Participants

The eligibility criteria for selecting participants were based on professional experience and geographical location. The study focused on a target population of IT project managers and leaders with three or more years of experience designing and implementing cloud-based applications within organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook. Chang et al. (2021) noted that the proper selection of participants is crucial for a quantitative analysis. Additionally, Stieninger et al. (2022) discussed the importance of carefully selecting individuals and ensuring their understanding of the vocabulary and terms used in the collection instrument to achieve the most accurate results. Stieninger et al. also argued that social media are an effective channel to make initial contact with the participants.

For the purpose of the current study, several strategies were used to find participants. Communication with potential participants was established through existing networking channels including work connections, social media platforms (primarily LinkedIn), and previous professional associations. Recruitment via electronic-based communication systems and social media is a commonly adopted method by researchers (Tella et al., 2020). This has been demonstrated in previous studies such as the one conducted by Shyam and Doddi (2019), who used Facebook to recruit participants for their survey on ML and non-ML techniques for cloud security, and Webb and Aly

(2020), who used online platforms to survey participants regarding the acceptance of VPCs.

I used networking connections in work environments and on social media to establish contact with potential participants. A relationship-building approach was taken, which involved contacting interested individuals via LinkedIn messaging, phone calls, and emails. Similar to the study of Ntambu and Adeshina (2021), participants were grouped into categories based on their professional experience and knowledge base, and trust and motivation were developed by emphasizing philanthropic objectives. Additionally, the language used in the email sent to the participants highlighted how the research would benefit them and others from a security perspective. The email ensured participants of data confidentiality, identity concealment, and the confidence provided by working under the trustworthy institution of Walden University. Stieninger et al. (2022) discussed the effectiveness of using social media for establishing initial contact and implementing a solid working relationship between the researcher and potential participants.

The selection of the participants was aligned with the purpose, research question, and hypotheses of the current study. According to Shyam and Doddi (2019), correctly identifying participants' relevant experience in their organizations is critical for answering the research question of a study. In the current quantitative study, participants were selected based on their experience as IT professionals working in cloud environments and their experience managing and supervising applications containing data, in which security and privacy are vital issues.

Research Method and Design

Method

Research methodology is the methodical and theoretical examination of techniques used in a specific field to create or enhance a scientific approach (Gupta & Gupta, 2022). In the current study, a quantitative method was chosen over qualitative or mixed methods because categorical answers to closed-ended questions were collected with an online survey. Greife and Maume (2020) noted that closed-ended questions provide a structured approach for understanding the relationships between dependent and independent variables.

Compared to qualitative studies, in which researchers analyze content with the aim of better understanding the why or what of a phenomenon (Kyngäs, 2020), quantitative methods are used to numerically measure the correlation between variables framed on the philosophy of positivism (Aburbeian et al., 2022). Qualitative studies are based on an iterative process used to analyze subject information and apply participant observations to produce an in-depth, coherent understanding of a given phenomenon (Mather et al., 2018). Aspers and Corte (2019) highlighted that qualitative research is an interpretative approach mixed with a naturalistic view of how individuals experience the world. Kyngäs (2020) noted that in a qualitative approach, conclusions are drawn by induction or abduction, while hypotheses are not postulated and, if postulated, are not tested within the underlying framework. In a quantitative approach, deductive reasoning is applied to test hypotheses addressing relationships between variables (Aburbeian et al., 2022). Because I analyzed the categorical answers of IT professionals with a focus on

assessing the relationship of PeS and PeP with the adoption of ML models in cloud environments, a quantitative approach based on an HLR was the most appropriate method. Additional (control) variables were considered to account for other factors that can affect the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type.

Mixed methods combine quantitative and qualitative approaches to draw comprehensive conclusions (Li et al., 2020). Fetters (2022) provided a categorization of mixed methods, comprising advanced designs, complex designs, embedded designs, intersected designs, and scaffolded designs. Because the purpose of the current study was to test the hypotheses in a positivist framework using quantitative methods, qualitative analysis was not applied, and therefore, mixed methods could not be implemented due to the lack of the qualitative component. Advanced, complex, embedded, intersected, and scaffolded mixed methods designs were not considered in this study.

Research Design

The research design of this study was based on the quantitative analysis of data collected through an online survey. The survey was completed by IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook. Pawar (2020) defined a research design as the process of collecting relevant data, and the techniques applied to facilitate the smooth scaling of the research operations yielding maximal information. According to Pawar, the

research design provides a structure for answering the research question and testing the hypotheses.

In the current study, the research objective was to examine the relationship between IT leaders' comprehension of project managers' PeS and PeP with the intent to use ML security models to secure data in cloud-based applications. To achieve the goal of this study, I collected primary data from the target population (IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions in South Loop in Chicago, University Park, and Oakbrook) based on their professional experience and their geographical location.

The data collection was based on nonprobabilistic sampling, and the data collection techniques included an online survey based on a 5-point Likert categorical scale. Due to the categorical nature of the independent and dependent variables, the data analysis methods involved the application of HLRs based on transformations of variables, similar to the studies of Rabe and Kostka (2024), Nambiar and Bolar (2023), and Chauhan et al. (2021), who applied a transformation of variables in the empirical application of the TAM. The HLRs applied to the data collected for the current study were used to estimate the correlations between the independent, dependent and control variables. Bloomfield and Fisher (2019) stated that correlational studies allow researchers to examine variable relations, providing a more bias-free observation. Correlational studies also provide researchers with the tools to infer whether the relationship in question is positive or negative. A positive correlation suggests that the variables

examined move in a similar direction, while a negative correlation suggests that variables move in opposite directions (Aburbeian et al., 2022). Li et al. (2020) noted that correlational studies could produce correlations that are statistically equal to zero, which indicates that the variables analyzed are unrelated. In the current study, a correlation research design was selected over other designs because the goal was to assess correlations between independent variables and a dependent variable. The purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications. The independent variables were PeS and PeP. The dependent variable was the adoption of ML models in cloud environments for securing data in cloud-based applications. Additional (control) variables were considered to account for other factors that can affect the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type.

Population and Sampling

The target population sampled in the study was IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions in the South Loop of Chicago, University Park, and Oakbrook. This target population aligned with the research question because the target population carried out duties in planning, facilitating, evaluating, and coordinating data security and privacy for cloud applications. This target population

comprised individuals considered to be middle management within IT organizations, as in the study conducted by Nassif et al. (2021). The characteristics of the target population in the current study also aligned with the research question because the target population (IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions in South Loop in Chicago, University Park, and Oakbrook) was directly responsible for the data privacy and security of applications in cloud environments. In addition, the target population of IT project managers and leaders was directly responsible for examining the benefits, challenges, and impact of implementing additional security measures and models in their organizations (see Tripathy et al., 2020). An IT organization is defined as any organization with a structured division that manages, handles, monitors, maintains, and establishes IT and information system services (Veloso et al., 2021).

The sampling method used in the current study was nonprobabilistic based on quota sampling. Nonprobability sampling methods use nonrandom criteria such as geographical proximity, expert knowledge, and the availability of the targeted individuals (Lah et al., 2020). Nonprobability sampling allows researchers to apply a more practical and conducive way of deploying surveys cost-effectively (Lah et al., 2020). The sampling method is also effective when the population is small because it allows all participants available to be invited at a small scale (Weng et al., 2021). A limitation of non-probabilistic sampling, however, is the potential generalization of the study results, because the results are limited to the group of interest analyzed.

The sample size for this study was determined through a power analysis performed with G*Power Version 3.1.9.7. G*Power is a statistical tool that is used to conduct power analysis through diverse testing options such as z tests, χ^2 tests, t tests, and F tests. Kang (2021) recommended the use of the F test family, specifically the HLR with R^2 deviation from zero models, for calculating the sample size based on known variables. In contrast, Cohen (1988) and Webb and Aly (2020) recommended a combination of a standard effect size equal to .5 and a power equal to .8 for the population effect (α), which represents the likelihood of rejecting the null hypothesis, as well as for the statistical power ($1-\beta$), which represents the likelihood of rejecting a false hypothesis. In the current study, the power analysis was based on an F -test model with an effect size α of .5 and error of .05, a power ($1 - \beta$) of .8 (80), and four predictors (PeP, PeS, and significant control variables: experience in cloud computing, and industry type). Additional control variables (respondent's education level, leadership roles, experience at the current position, and primary cloud computing strategy) were considered in the omnibus regression model. However, the only statistically significant control variables were the experience in cloud computing and industry type, so only those control variables were included. The results of the G*Power analysis suggested a minimum sample size of 84 IT professionals. After including the eight control variables, the required sample size decreased from 84 to 68. The actual study sample of 109 participants therefore exceeds the minimum requirement, ensuring sufficient statistical power (see Appendix A).

Ethical Research

Ethical research involves adhering to moral principles to protect research subjects and scientific values (Kumar et al., 2022). Similar to the research conducted by Aldahwan and Ramzan (2022), in the current study, the informed consent of the participants was ensured by establishing initial contact with potential participants and providing a straightforward consent and withdrawal process, data security statements, and agreement documents. Informed consent is a critical component of ethical research, and identifying a coherent consent process represents the foundation of the researcher's communication with participants (Kang, 2021). Furthermore, the informed consent process allows participants to make knowledgeable and voluntary decisions about whether to participate in a research study.

After selecting potential participants, an email was sent to initiate a transparent and prospective working relationship with the potential participants. The email contained an invitation to complete the survey and details about the consent process, as presented in Appendix B. The email also included a short overview of the topic, the purpose and goals of the survey, estimated completion times, and a list of supporting or participating institutes. Additionally, the email sent addressed the confidentiality and privacy of potential participants. The potential participants were presented with an informed consent document that included information about the data retention period, confidential information handling process, data access policies, and alternative options for withdrawing from the study.

The email sent to potential participants also clearly and coherently stated the withdrawal policy for potential participants, as shown in Appendix B. The withdrawal policy allowed potential participants to withdraw from the survey without their recorded information being stored. The withdrawal option would permanently delete all responses given by participants who decided to be excluded from the study. As shown in Appendix B, the survey included a withdrawal option to ensure compliance with ethical research guidelines. The right to withdraw is a critical research component helping to elevate trust in the research because it protects participants from an information imbalance, inability to hedge, and inherent uncertainty (Ferri et al., 2020). The email sent to potential participants explained that a request email would be required for the participant to be excluded from the survey, and a specific timeline was given in which participants could withdraw their information. Veloso et al. (2021) emphasized that a well-defined informed consent process and coherent participant procedures for withdrawing from the study are essential for avoiding ethical violations.

The email sent to potential participants also included a short description of the value of the research conducted and its potential positive impact on social change, environments, and innovation of information security. Neither monetary nor non-monetary incentives were provided for completing the online survey. The data collected with the online survey was stored in an encrypted medium, which was protected with a username and password to maximize participant confidentiality and security. The raw data collected for the study was stored offline on a separate storage device (USB disk) mirrored on another offline external solid-state drive. Both are held in a safe box for 5

years to comply with the Walden University Institutional Review Board guidelines. Raw data can be provided at the request of a participant within 5 years; however, the USB and data backup will be permanently deleted upon reaching the 5-year mark. As shown in Appendix B, the potential participants were presented with a statement explaining that the data collected would be retained for 5 years in an encrypted, password-protected utility. According to Webb and Aly (2020), data stored offline shall be protected and secured by utilizing a hashing algorithm or other security means to ensure participant anonymity and security. Microsoft Windows provides encryption utilities such as BitLocker (see Chkirbene et al., 2020), allowing users to encrypt entire volumes of data to help protect against unauthorized access or theft.

The study also adhered to ethical principles to ensure the privacy and confidentiality of participants. Nassif et al. (2021) described seven principles that should guide researchers in conducting ethical research: social and clinical value, scientific validity, fair subject selection, favorable risk-benefit ratio, independent review, informed consent, and respect for potential and enrolled subjects. The online survey adhered to these ethical guidelines by separately storing (with password protection) the consent forms, surveys, and other documents containing personal information. The confidentiality of participants was guaranteed by implementing techniques that protect personal details, such as age, gender, social security numbers, and identification numbers. To further guarantee the anonymity and confidentiality of the collected data, a code-based survey and reporting mechanism were employed to promote unbiased reporting. Veloso et al. (2021) emphasized the significance of ethical research, which must include a well-

defined informed consent process and coherent participant procedures for withdrawing from the study to avoid ethical violations. To ensure the protection of participants and organizations involved in this research, the data collected in this study was stored for 5 years in an encrypted password-protected offline utility, after which, the utility will be destroyed and disposed of accordingly. The Microsoft Windows security feature BitLocker was used to encrypt entire volumes of data to help protect them from unauthorized access or theft (see Chkirbene et al., 2020). The IRB approval number received from Walden University research ethics, compliance, and partnerships is 08-22-23-1017010.

Instrumentation

The instrument used in this study was an online survey, used to collect information on the perceptions of the target population (IT project managers and leaders with three or more years of experience designing and implementing cloud-based applications in organizations and institutions in South Loop in Chicago, University Park, and Oakbrook). According to Liu et al. (2021), online surveys provide participants with maximum privacy and comfort, promoting open information disclosure. Adeoye and Osibo (2023) conducted 121 surveys among various IT departments in Africa and found that cloud infrastructure had a significant impact on enterprise IT environments, therefore suggesting that adopting cloud infrastructure has numerous advantages, enabling companies to optimize their IT resources, access cutting-edge technology, and swiftly adapt to changing market demands. Stieninger et al. (2022) also pointed out that using

surveys as collection instruments allows researchers to analyze various factors impacting security decision-making within cloud infrastructures.

The online survey used in this study was an adaptation of the one used by Aburbeian et al. (2022), who provided permission to use the format of their survey (as shown in Appendix C). Aburbeian et al. evaluated the impact of different variables on the use of Metaverse technology by surveying 302 individuals between 20 to 60 years old who completed an education above high school. The survey conducted by Aburbeian et al. was based on a 5-point ordinal Likert scale, ranging from *strongly agree* to *strongly disagree*. As shown in Appendix D, the collection instrument included four items measuring PEOU, four items measuring PU, four items measuring attitude toward new technologies, and five items measuring the intention to adopt new technologies. Aburbeian et al. demonstrated the high validity and reliability of their instrument by conducting pilot tests, inviting experts from practical and academic domains, and revising the measurement criteria based on related literature. Aburbeian et al. applied Cronbach's alpha reliability methodology to evaluate the survey's internal consistency and coherence, obtaining a Cronbach's alpha coefficient of .82. The survey conducted by Aburbeian et al. (2022) was considered appropriate for this study because it was formulated in the framework of the TAM. According to Hanif and Lallie (2021), surveys framed on the TAM can help to evaluate the factors influencing the adoption of specific technologies.

The survey conducted by Aburbeian et al. (2022) was modified to fit the purpose of the current study, which was to examine the relationship between IT leaders'

comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications. The independent variables were PeS and PeP. Additional (control) independent variables were included to account for other factors that can affect the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. The online survey used to collect the information for this study comprised three parts and 39 questions. The survey addressed the qualifications of participants, the characteristics of their organizations, and their attitudes and perceptions regarding data privacy, data security, and ML security models.

The scale of measurement used for the survey answers was nominal and ordinal. The first part of the online survey contained questions with nominal answers regarding the qualifications of the participants in order to filter the sample and secure participants who complied with the professional requirements to participate in the study. According to Chang et al. (2021), beginning a survey with an assessment of the competency and qualifications of participants is critical for avoiding any discrepancies or ambiguities. Additionally, Braun et al. (2021) discussed the importance of selecting competent participants who have an appropriate amount of knowledge in the field of study to ensure validity and avoid biased data.

The second part of the online survey included nine questions with answers based on an ordinal scale (5-point Likert scale). This section collected information regarding the characteristics of participants and their organizations. Navaei and Tabrizi (2022)

highlighted the importance of sampling individuals with similar characteristics for ensuring the generalizability and validity of the research. The final part of the online survey contained 28 closed-ended questions based on a 5-point Likert scale, similar to the study conducted by Aburbeian et al. (2022). Specifically, the Likert scale used in the survey was divided into the following five categories: (1) strongly disagree, (2) disagree, (3) neither agree nor disagree, (4) agree, and (5) strongly agree. Ntambu and Adeshina (2021) argued that surveys are a practical data-collection method for examining relationships and correlations between variables.

In the online survey used to collect information on the perceptions of IT professionals, both the dependent variable (adoption of ML models) and the independent variables (PeS and PeP) were measured as categorical variables with a 5-point ordinal Likert scale. This was a modification of the survey developed initially by Aburbeian et al. (2022), made to adapt the survey to the research question and hypothesis of this study. Kang (2021) explained that research instruments can be modified or extended to capture specific information about individuals participating in a different study. Chang et al. (2021) noted that reusing data collection instruments provides researchers with a flexible, efficient, and tested approach for collecting data to fit their own specific goals.

The survey participants' answers were used to gain an understanding of the relationship between the dependent and independent variables of the study. Specifically, closed-ended questions with no follow-up were formulated to examine the correlation of IT managers' PeS and PeP with the adoption of ML security models in cloud environments. The questions were formulated using technical but simple and coherent

language. This approach is appropriate for measuring the variables measured by the instrument (adoption of ML models, PeS and PeP), as ordinal questions help to capture the range of possible perceptions of the respondents. During the modeling stage, the categorical answers were converted to numerical score through dichotomization (see the Data Analysis section for details). The instrument used to collect the answers from respondents is shown in Appendix D. The collected data are available upon request.

Data Collection Technique

A self-administered online survey was chosen as the data collection technique in this study. SurveyMonkey, a web-based tool, was used to distribute the survey and collect the answers of the participants. Online surveys are a cost-effective and flexible way of collecting information and ensuring maximum reach (Al-Madhagy Taufiq-Hail et al., 2021). With the growing use of remote online tools, web-based surveys have become one of the most widely implemented approaches for collecting data in quantitative studies (Shyam & Doddi, 2019).

The main advantage of online surveys is time-saving for users and researchers, because both parties can communicate and complete their tasks asynchronously (Tripathy et al., 2020). Additionally, online surveys are cost-efficient because they require less effort to prepare and administer, resulting in a faster data collection times (Stieninger et al., 2022). Online surveys can also significantly increase the response rates of participants (Webb & Aly, 2020). However, the asynchronous nature of online surveys may be a disadvantage if it causes respondent cooperation issues, limited population access, or reduced data reliability (Stieninger et al., 2022).

After identifying potential participants within the target population (IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook), the LinkedIn platform was used as the primary tool for inviting and recruiting the participants of the study. The initial invitation email included a description of the study and an invitation to participate by completing an online survey. Braun et al. (2021) argued that online questionnaires provide an open and flexible environment to address a wide range of research questions and collect data relating to people's views, experiences, or material practices, through representational or meaning-making practices.

After the potential participants agreed to take part in the study, they received a consent form email containing all necessary ethical research components, such as data confidentiality, withdrawal policy, risks, benefits, and the time required to complete the survey. Links to the online survey were then sent to all participants after they provided their signed consent. Liu et al. (2021) highlighted the importance of providing consent forms for participants. Consent forms help protect the researcher, the institution, and the participants, ensuring autonomy, privacy, security, and confidentiality.

Data Analysis

Research Question and Hypotheses

Is there a relationship between IT leaders' comprehension regarding project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications, after controlling for respondents' education level, leadership roles,

experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type?

The null hypothesis (H_0) of the study posited that there is no statistically significant relationship between IT leaders' comprehension regarding project managers' PeS and PeP with their intent to implement ML security models for securing data in cloud-based applications, after controlling for the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type?

The alternative hypothesis (H_1) posited that there is a statistically significant relationship between IT leaders' comprehension regarding project managers' PeS and PeP with their intent to implement ML security models for securing data in cloud-based applications, after controlling for the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. As suggested in H_1 , IT leaders' comprehension of project managers' PeS and PeP may significantly influence their decisions to implement ML security models. The comprehension of these factors may play a vital role in determining their adoption of ML-based security solutions for securing their cloud-based applications' data.

Statistical Analysis

Because both the dependent and independent variables of the study were categorical (non-numerical), methods such as linear regression based on ordinary least squares (OLS), analysis of variance (ANOVA), and t tests were not suitable to answer the

research question and test the hypothesis of the study. Calver and Fletcher (2020) argued that ANOVA is not suitable for categorical data, and Walters (2021) highlighted that although the t test is widely used, it is not appropriate in all cases, such as when the level of measurement is not continuous. Linear regression based on OLS, ANOVA and t tests is typically used with the assumption that dependent variables are numerical and continuous from a Gaussian (normal) distribution (Knief & Forstmeier, 2021). In the current study, however, the perceptions of IT professionals were captured with a Likert scale that produces categorical and discontinuous dependent and independent variables that do not follow a normal distribution. ANOVA relies on separating observed variant data into distinct components by comparing the means of a continuous variable with two or more independent ones (Lah et al., 2020). The family of ANOVA tests (one-way ANOVA, two-way ANOVA, and N-way ANOVA) and t tests evaluate the equality of the means of the dependent variable across groups (Kang, 2021). However, because the dependent variable in the current study was a categorical (non-numerical) variable, the means could not be calculated (see Walters, 2021). Thus, ANOVA tests and t tests could not be used to answer the research questions and test the hypothesis of the current study.

Due to the categorical nature of the dependent and independent variables of the study, an HLR analysis was used to analyze the relationship between the IT leaders' comprehension regarding IT project managers' PeS and PeP with the adoption of ML models in cloud environments after controlling variables. These transformations were applied in previous studies, such as those of Rabe and Kostka (2024), Nambiar and Bolar (2023), and Chauhan et al. (2021), in the empirical application of the TAM. Generalized

MLR models have many advantages over traditional regression based on OLS, ANOVA, or t tests, namely that the dependent variable does not need to have a normal distribution, and that optimal estimators can be obtained with maximum likelihood. As highlighted by Pardo (2020), functions that transform the dependent variable but still apply a linear multiple regression model in the equation of the explanatory variables lead to generalized linear models. These types of generalized linear models have been previously used by Isautier et al. (2020) and Narayana et al. (2020) to analyze the perceptions of individuals.

In the current study, the use of HLR allowed for the estimation of the relationship between IT leaders' comprehension of PeS and PeP with the adoption of ML models in cloud environments after control variables. While correlational analysis assesses whether there is a relationship between two variables; HLR allows for examining these relationships while controlling for confounding factors (Lah et al., 2020). Based on the sign of the correlation coefficient, researchers can determine the direction of the relationship between two or more variables (Jha & Sharma, 2021).

HLR models also provide inferential statistics for testing the hypothesis of the study, which helps to infer whether the null hypothesis can be rejected (Nadeem & Lee, 2020). Let Y_i be the dependent variable (adoption of ML security models in cloud-based apps), which is equal to 1 if any of the $i = 1, 2, \dots, n$ respondents of the online survey agreed or strongly agreed with the five items used survey to calculate the dependent variable, and 0 if the respondents were neutral or disagreed with the items:

$$Y_i = \begin{cases} 1 & \text{if the } i\text{-respondent agrees/strongly agrees about adopting ML models in cloud environments} \\ 0 & \text{if the } i\text{-respondent is neutral/disagrees about adopting ML models in cloud environments} \end{cases}$$

The distribution of Y_i indicates the probability $P(Y_i=1)=\pi$ of adopting ML models in cloud environments, and the probability $P(Y_i=0)=(1-\pi)$ of not adopting ML models in cloud environments. Potential explanatory variables (the main effects of interest: PeS and PeP) and control variables (the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type) can be included to aid in understanding which variables are related to the probability of adopting ML models in cloud environments. Let Z_{1i} and Z_{2i} be the potential explanatory variables of ML adoption in cloud environments, specifically PeP (Z_{1i}) and PeS (Z_{2i}). Given the expected value of Y_i , $\mu=E(Y_i)$, the link function will be a function $g(\cdot)$ that relates μ to the main effects Z_{1i} , Z_{2i} and to the $1, 2, \dots, k$ control variables X_1, X_2, \dots, X_k (see Pardo 2020) in a linear equation with multiple regressors:

$$g(\mu) = \alpha + \beta_1 Z_{1i} + \beta_2 Z_{2i} + \dots + \gamma_1 X_{1i} + \gamma_2 X_{2i} + \dots + \gamma_k X_{ik}$$

β_1 and β_2 are the parameters that measure, respectively, the influence of the comprehension of PeP (Z_{1i}) and PeS (Z_{2i}) on the adoption of ML security in cloud-based apps; γ_k are $1, 2, \dots, k$ parameters that measure the importance that each control variable X_1, X_2, \dots, X_k has for the variability in $E(Y_i)$ and α is a constant (the intercept) in the linear equation: $\alpha + \beta_1 Z_{1i} + \beta_2 Z_{2i} + \dots + \gamma_1 X_{1i} + \gamma_2 X_{2i} + \dots + \gamma_k X_{ik}$.

The HLR analysis was conducted using PeP, PeS and Intent to use ML security models after controlling the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. The findings revealed that, across all models, PeP and PeS were significant predictors of intent to use ML security models, with PeS consistently making a higher

contribution for education level ($\beta=-.012$, $p=.895$), leadership roles ($\beta=.141$, $p=.122$), experience at current position ($\beta=-.081$, $p=.292$), primary cloud computing strategy ($\beta=-.060$, $p=.458$), experience in cloud computing ($\beta=-.230$, $p=.003$), and industry type ($\beta=.442$, $p=.000$). Moreover, education level, leadership roles, experience at the current position, and primary cloud computing strategy did not significantly explain the variance in the dependent variable, intent to use ML security models ($\beta=-.012$, $p=.895$), ($\beta=.141$, $p=.122$), ($\beta=-.081$, $p=.292$), ($\beta=-.060$, $p=.458$), respectively, confirming that none of these control variables significantly influenced the intent to use ML security models. Furthermore, the analysis highlighted that cloud computing experience, and industry type were significant predictors of intent to use ML security models ($\beta=-.230$, $p=.003$), and ($\beta=.442$, $p=.000$) respectively. However, when PeP and PeS were included in the regression models, the explained variance improved significantly, achieving an R^2 of .536. The model with eight predictors, including PeP and PeS, yielded $F(8, 97) = 14.006$, $p=.000$, indicating that these factors collectively explained 53.6% of the variance in intent to adopt ML security models.

Data Cleaning and Screening

Performing data cleaning and editing throughout the research process is essential for ensuring accurate results and identifying and adjusting for potential errors, as well as for reviewing datasets for invalid, inconsistent, missing, or outlier data (Nassif et al., 2021). Data cleaning is also crucial for producing valid, reliable, and generalizable results by resolving inconsistencies (Frazer et al., 2022). In this quantitative study, data cleaning methods were implemented to maintain data integrity and remove any data outliers within

the datasets. Furthermore, researchers often encounter a lack of complete and responsive survey submissions, resulting in missing data (Jha & Sharma, 2021). To address this problem, in this study, several procedures were used to screen and tag participant responses with incomplete or inaccurate data. The techniques used for data cleaning and handling outliers included removing duplicate and irrelevant data, implementing clear and consistent formatting, and checking for errors within the survey.

A data quality check was also performed to evaluate missing data, inconsistencies, and outliers. Lee and Nadim (2020) discussed the importance of checking for missing or blank data in datasets and analyzing the appropriateness of imputing the data. Furthermore, Musyaffi and Arinal (2021) discussed the importance of cross-checking responses between related questions and/or different data sources to check for any inconsistencies in datasets. Lee and Nadim (2020) also argued that checking for any extreme values can help expose outliers in a dataset. Although no missing values or outliers were identified, the outcome variable was binarized to reflect adoption intent more clearly. This transformation was purposeful modeling decision to align with the requirements of model and not due to data loss or quality issues.

Testing Assumptions

A critical examination of assumptions is essential for ensuring the accuracy of research results. Any violations of these processes can lead to biases, wide confidence intervals, and ambiguous conclusions (Kang, 2021). Multiple regression models based on OLS are based on the assumptions that the relationship between variables is linear,

dependent variables are continuous, data has homoscedasticity, there are no spurious outliers, and the error is normally distributed (Weng et al., 2021).

Multicollinearity is an additional issue that may arise if the potential explanatory variables are strongly correlated, which can lead to significantly inaccurate results (Kang, 2021). Therefore, detecting the presence of multicollinearity is critical for properly testing the hypothesis of the study. Multicollinearity can be evaluated using variance inflation factors (VIFs), which allow researchers to measure the strength of the correlation between independent variables (Weng et al., 2021). VIFs below a value of 10 indicate that multicollinearity is less likely (Weng et al., 2021). Multicollinearity can be mitigated by removing the affected variables or implementing a different regression analysis variant (Kang, 2021).

Interpreting Inferential Results

A Hierarchical Linear Regression analysis was conducted to assess the significance of PeS and PeP after controlling for respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type among the sample of IT project managers and leaders of South Loop of Chicago, University Park, and Oakbrook. Intent to use ML security models was the dependent variable. Preliminary assumptions of multicollinearity, outliers, normality, linearity, homoscedasticity, and independence of residuals were assessed, and no violations were noted.

Statistical Software

In this study, IBM SPSS, Version 27.0 for a Windows 64-bit OS, was used to analyze data and produce descriptive and inferential statistics. SPSS is a statistical software that is popular among researchers due to its robustness, effectiveness, and reliable functionality (Chang et al., 2021). According to Chang et al., SPSS is widely used in social science research due to its descriptive and inferential statistics capabilities and its user-friendly interface, helping to minimize errors and provide efficient calculations.

Study Validity

Validity is a critical component of quantitative studies, indicating that the data collection instruments are effective and precise in measuring what they are intended to measure (Tripathy et al., 2020). There are different types of validity: face validity, which evaluates if the instrument measures what it is supposed to measure; content validity, which evaluates if the instrument covers the full range of the concepts of interest; and construct validity, which evaluates whether the instrument captures the underlying theoretical constructs of the study. Pilot testing, expert reviews, statistical analyses, and comparing results with established measures are common approaches for evaluating validity, but no instrument is perfectly valid (Kalkbrenner, 2021).

Threats to External Validity

Findley et al. (2021) define *external validity* as the extent to which inferences drawn from a sample in a study can apply to a broader population or other target populations. External validity allows researchers to measure the ability of the study

outcomes to be expanded and generalized for a broader population (Tella et al., 2020). Due to the non-probabilistic sample strategy chosen in the current study, the validity was circumscribed to the target population of interest (IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions in South Loop in Chicago, University Park, and Oakbrook). To reduce selection bias, predefined screening methods were applied to ensure proper recruitment of the target group of interest. In their study, Lotfaliany et al. (2022) used screening methods to reduce the risk of sampling bias. This strategy was also utilized in this quantitative study to reduce potential bias that can be caused by not considering the proper characteristics of the target group of interest.

Threats to Internal Validity

Internal validity can influence the reliability and credibility of a study. Internal validity pertains to whether the study design, conduct, and analysis properly answer the research questions, without bias (Fitzpatrick & Stefan, 2022). Since the current study was based on a correlational research design that is not experimental, there was no significant risk to internal validity.

Threats to Statistical Conclusion Validity

Statistical conclusion validity refers to the degree to which conclusions and observations regarding the relationship between variables are reasonable, in terms of the effect size, sampling technique, measurement and instrument methods, and the statistical tests used in the study (Weng et al., 2021). Effect sizes help to demonstrate the significance of the statistically significant results obtained in a study, because effect sizes

measure the magnitude of the difference of variables of interest across groups and the magnitude of the relationship between variables (Kang, 2021). The current study addressed the potential threats to statistical conclusion validity and the effect size by pre-calculating an optimal sample size for a Type I error rate equal to 5% and a statistical power of 80%. A non-probabilistic sampling quota strategy was used to obtain a sample size equal to or higher than the one needed for statistical validity. The constructs and measurements were also properly defined in the collection instrument to ensure that the desired main effects of interest (relating to PeP and PeS) were properly captured by the items of the survey.

Rationale for Generalizing Findings to a Larger Population

Generalizability refers to the degree to which the results of a study can be applied in a broader context and to a population that is different from the one for which the sample was selected (Lah et al., 2020). The results of the current study were applicable for the target group of interest (IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions in cloud environments in South Loop in Chicago, University Park, and Oakbrook), due to the non-probabilistic sample strategy chosen for the study. Generalizability differs in quantitative research and qualitative research. Researchers conduct qualitative studies to gain a rich understanding of a topic within a specific group, while quantitative studies allow for broader applicability and statistical inference. The generalizability of qualitative studies is lower compared to quantitative studies, according to Aspers and Corte (2019) and Li et al. (2020). External validity is a

more relevant concern in quantitative studies, as it refers to whether findings can be applied in different settings or to different populations. In the current study, the limitations of generalizability were related to the sampling method, as random sampling methods increase generalizability compared to non-probabilistic convenience sampling of volunteers.

Transition and Summary

This section included details about the quantitative correlational approach applied to evaluate the relationship of the adoption of ML security models (dependent variable) with two independent variables: (a) the perceptions of IT professionals about data security in cloud environments, and (b) the perceptions of IT professionals about data privacy in cloud environments. In this section, the data collection methods were described, as well as the instrument used to collect the information of the target population (IT leaders and managers who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook). Additionally, the rationale and the suitability of the statistical analysis were explained, as well as potential threats to the validity and generalizability of the study.

Section 3 will include the results of the study, following an analysis of the collected data and a testing of the hypothesis of the study. Section 3 will also include the implications of the study for social change, recommendations for future research, and a summary and conclusion.

Section 3: Application to Professional Practice and Implications for Change

Section 1 included details about the background, the theoretical framework (TAM), the research question, and the hypotheses of the study. Section 2 contained descriptions of the data collection methods, the instruments and statistical tools used to analyze the data, and the potential threats to validity and generalizability. In Section 3, the findings of the study are presented, as well as the implications of the results for social change and application for professional practice. In addition, recommendations for action and further research, reflections, and a conclusion are provided at the end of this section.

Overview of Study

The purpose of this quantitative correlational study was to examine the relationship between IT leaders' comprehension regarding IT project managers' PeS and PeP with the intent to adopt ML models for securing data in cloud-based applications. The independent variables were PeS and PeP. The dependent variable was the adoption of ML models in cloud environments for securing data in cloud-based applications. The target population was IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook. Additional (control) independent variables were considered to account for other factors affecting the adoption of ML models in cloud environments. The control variables were the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. The results of hierarchical linear regression of block one were statistically significant $F(6,$

99)=8.011, $p=.000$, $R^2 =.327$ explaining the only 32.7% of the variance in intent to adopt ML security models. PeP and PeS were included in block 2. Two predictors, PeP and PeS entered in block 2, explained 53.6% of the variance ($F(8, 97) =14.006$, $p < .001$), education level ($\beta=-.012$, $p=.895$), leadership roles ($\beta=.141$, $p=.122$), experience at current position ($\beta=-.081$, $p=.292$), and primary cloud computing strategy ($\beta=-.060$, $p=.458$) were not significantly predictors. In contrast, experience in cloud computing ($\beta=-.230$, $p=.003$), and industry type ($\beta=.442$, $p=.000$) were significant. These results emphasize the critical role of PeP and PeS as primary determinants of intent to use ML security models.

Presentation of Findings

In this section, statistical evidence is provided to test the hypotheses and answer the research question of the study.

Descriptive Statistics

A total of 113 participant answers were obtained in the online survey, but seven answers were not analyzed due to the participants having fewer than three years of professional experience. The remaining sample of 106 respondents contained the answers of IT professionals with three or more years of experience (see Table 2).

Table 2
Professional Experience in Cloud Computing

Experience (years)	Frequency	Percentage	Valid percentage	Cumulative percentage
1–3	7	6.6%	6.6%	6.6%
3–5	24	16.0%	16.0%	22.6%
More than 5	82	77.4%	77.4%	100%
Total	106	100%	100%	

In the online survey, five statements were used to calculate the dependent variable (adoption of ML security models in cloud-based apps): (a) I tend to use ML security models in my cloud-based apps, (b) I increase the occurrences of using ML security models in my cloud-based apps, (c) I use ML security models in my cloud-based apps helps to enhance security, (d) I'd love to use ML security models in my cloud-based apps, and (e) I use ML security models to provide elevated security to my cloud-based apps. The dependent variable was calculated as a binary variable equal to 1 if the respondent agreed or strongly agreed with the statements presented in the survey and 0 if the respondent was neutral, disagreed, or strongly disagreed with the statements.

Binarization was applied to the ordinal responses due to the high concentration of answers in the favorable categories *agree/strongly agree* (see Tables 2 to 6). Although the dataset contained no missing values or outliers, the response distribution was highly skewed, with very few observations in the neutral or disagree categories. This skewness limited the feasibility of using ordinal regression model, as they require sufficient data across all response categories. Using ordinal models under these conditions could have

reduced degrees of freedom and potentially led to unreliable estimates. Therefore, I used binarization to combine the responses into two categories: those who agreed or strongly agreed with the statements regarding using ML security models in cloud-based apps, and those who were neutral or disagreed with the statements regarding using ML security models in cloud-based apps.

Table 3***Item 1 Used for DV Calculation***

Participant response	Frequency	Percentage	Valid percentage	Cumulative percentage
Strongly agree	66	62.3%	62.3%	62.3
Agree	36	34.0%	34.0%	96.2%
Neutral	4	3.8%	3.8%	100%
Total	106	100%	100%	

Note. Item 1 used to calculate the dependent variable: I tend to use ML security models in my cloud-based apps.

Table 4***Item 2 Used for DV Calculation***

Participant response	Frequency	Percentage	Valid percentage	Cumulative percentage
Strongly agree	57	53.8%	53.8%	53.8%
Agree	45	42.5%	42.5%	96.2%
Neutral	4	3.8%	3.8%	100%
Total	106	100%	100%	

Note. Item 2 used to calculate the dependent variable: I increase the occurrences of using ML security models in my cloud-based apps.

Table 5***Item 3 Used for DV Calculation***

Participant response	Frequency	Percentage	Valid percentage	Cumulative percentage
Strongly agree	52	49.1%	49.1%	49.1%
Agree	48	45.3%	45.3%	94.3%
Neutral	6	5.7%	5.7%	100%
Total	106	100%	100%	

Note. Item 3 used to calculate the dependent variable: I use ML security models in my cloud-based apps to enhance security.

Table 6***Item 4 Used for DV Calculation***

Participant response	Frequency	Percentage	Valid percentage	Cumulative percentage
Strongly agree	50	47.2%	47.2%	47.2%
Agree	47	44.3%	44.3%	91.5%
Neutral	8	7.5%	7.5%	99.1%
Disagree	1	.9%	.9%	100%
Total	106	100%	100%	

Note. Item 4 used to calculate the dependent variable: I'd love to use ML security models in my cloud-based apps.

Table 7***Item 5 Used for DV Calculation***

Participant response	Frequency	Percentage	Valid percentage	Cumulative percentage
Strongly agree	43	40.6%	40.6%	40.6%
Agree	51	48.1%	48.1%	88.7%
Neutral	11	10.4%	10.4%	99.1%
Strongly disagree	1	.9%	.9%	100%
Total	106	100%	100%	

Note. Item 5 used to calculate the dependent variable: I use ML security models to provide elevated security to my cloud-based apps.

Other descriptive statistics such as the mean and standard deviation did not apply to the collected data of the study because the dependent variable and the independent variables were nominal (categorical).

Test of Assumptions

A Hierarchical Linear Regression analysis was conducted to assess the significance of PeS and PeP after controlling for respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. PeP and PeS were the predictor variables. The dependent variable was the intent to use ML security models. The target population was IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook.

Preliminary analyses were conducted to ensure that the assumptions of multiple regression were met prior to performing the hierarchical multiple regression analysis. Specifically, linearity, normality, homoscedasticity, independence of residuals, and multicollinearity were assessed. Linearity and homoscedasticity were evaluated through scatterplots of standardized predicted values versus standardized residuals. Normality of residuals was examined through a histogram and normal probability (P–P) plot. Independence of residuals was evaluated using the Durbin–Watson statistic. Multicollinearity was assessed using variance-inflation factor (VIF) and tolerance values, and potential outliers were examined using Cook's distance and Mahalanobis distance.

Examination of the standardized residual scatterplot indicated a random dispersion of points around the zero line, supporting the assumptions of linearity and homoscedasticity. The histogram of standardized residuals ($M \approx 0$, $SD = 0.97$, $N = 106$)

demonstrated a distribution that closely approximated the normal curve, and the normal P–P plot confirmed that residuals followed the expected diagonal pattern, indicating that the assumption of normality was satisfied. The Durbin–Watson statistic was 2.05, confirming independence of residuals. Multicollinearity diagnostics revealed acceptable values, with variance-inflation factors (VIFs) ranging from 1.18 to 1.39 and tolerance values between .715 and .846, all well within recommended thresholds (VIF < 5.0, tolerance > .20).

Outlier diagnostics indicated a maximum standardized residual of 3.779, Cook’s-distance values below 1.0, and no Mahalanobis-distance values exceeding the critical $\chi^2(8) = 26.12$, $p < .001$. These findings confirmed the absence of influential cases or high-leverage points. Collectively, the results verified that the dataset met all assumptions required for hierarchical multiple regression and was suitable for inferential analysis.

Inferential Results

A Hierarchical Linear Regression analysis was conducted to assess the significance of PeS and PeP after controlling for respondents’ education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type. PeP and PeS were the predictor variables. The dependent variable was the intent to use ML security models. The target population was IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook. Preliminary analysis was conducted to

assess the assumption of multicollinearity, outliers, normality, linearity homoscedasticity and independence of residuals; no violations were noted.

Education level, leadership roles, experience at current position, experience in cloud computing, primary cloud computing strategy, and industry type were entered at block one, and the results of hierarchical linear regression were statistically significant $F(6, 99)=8.011, p=.000, R^2=.327$ explaining the only 32.7% of the variance in intent to adopt ML security models. PeP and PeS were included in block 2. They explained 53.6% of the variance in intent to adopt ML security models $F(8, 97)=14.006, p=.000, R^2=.536$ indicating that the model could explain 53.6% of the variance in intent to adopt ML security models. Both predictors provided a significant contribution to the model, with PeS ($\beta=.338, p=.000$) providing a slightly higher contribution than PeP ($\beta=.224, p=.011$). These results indicate that education level ($\beta=-.012, p=.895$), leadership roles ($\beta=.141, p=.122$), experience at current position ($\beta=-.081, p=.292$), and primary cloud computing strategy ($\beta=-.060, p=.458$) were not significantly predictors. In contrast, experience in cloud computing ($\beta=-.230, p=.003$), and industry type ($\beta=.442, p=.000$) were significantly predict intent to use ML. The null hypotheses is rejected, and the alternative hypotheses is accepted. Table 8 shows the descriptive statistics and table 9 shows the regression summary.

Table 8

Descriptive Summary of HLR

<i>Variables</i>	<i>Mean</i>	<i>Std. Deviation</i>
Intent to use ML	1.7340	.41470

Education level	5.6038	.59649
Leadership roles	2.9434	1.59660
Experience at Current Position	2.5094	.95862
Experience in cloud computing	3.7075	.58500
Primary Cloud computing model strategy	2.2925	.98529
Industry Type	4.1415	2.65631
PeP	1.6085	.38886
PeS	1.6297	.37675

Table 9***Regression Summary of HLR***

<i>Variable</i>	β	<i>SE B</i>	<i>Beta</i>	<i>Sig</i>	R^2	ΔR^2	LL	UL
Step 1				.000	.327	.327		
Education Level	-.013	.076	-.018	.868			-.164	.138
Leadership Roles	.049	.028	.191	.078			-.006	.105
Experience at Current Position	-.047	.039	-.108	.237			-.125	.031
Experience in Cloud Computing	-.137	.064	-.194	.035			-.264	-.010
Primary Cloud Computing Strategy	.053	.037	.126	.154			-.020	.126
Industry Type	.072	.015	.463	.000			.042	.103
Step 2				.003	.536	.209		
Education Level	-.008	.064	-.012	.895			-.135	.118
Leadership Roles	.037	.023	.141	.122			-.010	.083

Experience at Current Position	-.035	.033	-.081	.292		-.101	.031
Experience in Cloud Computing	-.163	.054	-.230	.003		-.271	-.056
Primary Cloud Computing Strategy	-.025	.034	-.060	.458		-.092	.042
Industry Type	.069	.013	.442	.000		.043	.094
PeP	.239	.092	.224	.011		.056	.421
PeS	.372	.090	.338	.000		.193	.551

Theoretical Discussion of Findings

As mentioned in Sections 1 and 2, the theoretical framework of this study is the TAM, which was developed by Davis (1989). The framework helps to explain the adoption of new technologies with factors including PU and PEOU (Hatmawan & Taufiq, 2021). Nevertheless, the TAM framework is used with the knowledge that additional variables may influence technology acceptance, and therefore, researchers can incorporate these additional variables into the model to gain a more comprehensive understanding of the drivers of technology acceptance in specific contexts (Musyaffi & Arinal, 2021). In the current study, PeP and PeS were found to be relevant factors affecting the adoption of ML models in cloud environments, alongside additional control variables (the respondents' education level, leadership roles, experience at the current position, experience in cloud computing, primary cloud computing strategy, and industry type). These inferential results align with those of Hanif and Lallie (2021) and Siagian et al. (2022), who found that PeP and PeS were significant predictors of consumer behavioral intentions on payment platforms and mobile banking applications.

The results of this study indicate that comprehension regarding the perceptions of IT professionals is a crucial factor in achieving security and privacy goals in hybrid cloud networks. These results complement the findings of the systematic review conducted by Nassif et al. (2021), who highlighted the pivotal role that ML plays in enhancing security and privacy in cloud environments. This alignment of the results with those of previous studies strengthens the evidence that PeP and PeS are relevant for the adoption of new technologies aimed at enhancing cloud security and privacy.

The findings of this study also support the conclusions drawn by Shyam and Doddi (2019) and Stieninger et al. (2022), who highlighted the effectiveness of ML techniques in enhancing cloud security and privacy and argued that data privacy and data security concerns influence the adoption of new technology in an organization. Tripathy et al. (2020) noted the effectiveness of ML security models in mitigating Structured Query Language injection attacks. Thus, the results of this study indicate that changing the perceptions of IT leaders and managers is integral for establishing ML solutions to address specific security threats, such as dynamic intrusion detection (see Chkirbene et al., 2020).

The results of this study do not align completely with those of Butt et al. (2020), who found that only PeS, and not PeP, is a relevant factor in cloud computing. In contrast with the results of Butt et al. (2020), in this study, the values of the maximum likelihood estimates equal $\hat{\beta}_1 = .224$ for PeP and $\hat{\beta}_2 = .338$ for PeS, indicating that the perception of data security is more relevant than the perception of data privacy for the adoption of ML security models in cloud environments, since $\hat{\beta}_1 < \hat{\beta}_2$ (see Table 9). This discrepancy

with the results of Butt et al. (2020) can indicate that the influence of PeS and PeP may vary depending on the organizational context and the specific use cases and applications within the cloud security domain.

In summary, the alignment of the findings of this study with previous studies indicates that IT leaders' comprehension regarding project managers' PeP and PeS has a critical influence on the adoption of ML models in cloud environments. The differences between the current study and other studies may be related to context-specific applications in cloud computing.

Application to Professional Practice

Using the results of this study, IT leaders can promote enhanced cloud environments to their IT professionals by encouraging positive perceptions of the technology and highlighting the benefits of implementing ML models. Thus, the results of this study may have a positive influence on the security and privacy of cloud deployment strategies by promoting the adoption of ML models. Furthermore, by recognizing the importance of addressing security and privacy concerns, IT managers and leaders can make more informed decisions regarding which ML models to implement and how to integrate the models into their systems. This proactive approach can help organizations to better protect data and ensure the reliability of ML-driven initiatives.

The findings of the study are also applicable to professional practice in terms of risk management and regulatory compliance within the IT industry. IT managers and leaders must navigate a complex landscape of data protection regulations and cybersecurity threats. Understanding the positive impact of PeS and PeP on the

implementation of ML security models can guide IT leaders in aligning their strategies with best practices and compliance standards at the industry level. These strategies can help organizations to mitigate risks associated with data breaches and non-compliance, as well as to avoid financial and reputational consequences.

The insights gathered from the results of this study can provide additional guidance for IT managers and leaders in allocating resources effectively. Understanding the positive influence that the comprehension of PeP and PeS has on the adoption of ML models allows organizations to prioritize technologies and strategies that address these critical factors. Investments in these technologies ensure that resources are directed towards initiatives with a higher likelihood of success, optimizing budget allocation and resource utilization. Managers can thus make more compelling cases for requesting additional resources by highlighting the tangible benefits of improving the perceptions of IT professionals about data security and privacy.

The results of this study can also be used to provide a performance evaluation framework for IT professionals. IT managers and leaders can incorporate metrics related to security and privacy considerations in the performance evaluation criteria of ML deployments. These metrics provide accountability benefits, allowing organizations to foster a result-driven culture that places a premium on safeguarding data and upholding privacy standards.

The findings of the study can also influence how IT managers and leaders evaluate technology and collaborate with technology vendors in practice. When selecting ML security solutions or implementing vendor-based partnerships, organizations can

prioritize those demonstrating a stronger commitment to security and privacy. IT managers and leaders can use the results of this study as benchmarks to assess the alignment of potential vendors with the criteria provided. This approach will enhance the protection of data and foster trust and transparency between organizations and their technology partners, thus contributing to more successful and secure ML deployments.

In conclusion, the findings of this study can be applied to various facets of professional practice within the IT domain. From strategic decision-making and resource allocation to risk mitigation and employee accountability, the findings can empower IT managers and leaders to navigate the complexities of ML solutions more effectively, ultimately contributing to the promotion of enhanced data security and privacy in the cloud environments of their organizations.

Implications for Social Change

The findings of this study help to shed light on the impact of the perceptions of data security and data privacy on the adoption of ML models in cloud environments. These results can increase the rate of automation of data security and privacy in cloud-based applications, which will play a pivotal role in enhancing privacy and security awareness among individuals and organizations. This awareness would lead to more responsible data-handling practices, fostering an overall culture of privacy and security.

As the digital landscape continues to evolve and PII becomes more prevalent, the importance of securing personal and private data cannot be overstated. By showcasing the positive influence of PeS and PeP on the adoption of ML models, this research underscores the critical role of data privacy and security considerations for technology

adoption. In an era characterized by increasing data breaches and privacy concerns, this study can empower data subjects (individuals whose PII is collected) by advocating for stronger safeguards. When individuals are aware that an organization prioritizes the security and privacy of their data, they are more likely to entrust their data and information to that organization. Fostering trust is essential for promoting the growth of digital services, e-commerce, and other data-driven innovations. Consequently, this research contributes to the promotion of a social shift in which individuals have greater confidence in cloud environments for protecting their personal information.

The findings of the study emphasize the responsibility of organizations to safeguard PII. In today's data-centric world, businesses collect vast amounts of personal information for various purposes. As underscored in this research, organizations should prioritize security and privacy in their technological initiatives to promote the adoption of new ML technologies, comply with regulations, and uphold their social responsibility. This shift towards responsible data stewardship can result in a more ethical and trustworthy business environment where companies actively protect the PII of their customers.

The implications of this study also extend to the realm of legislation and regulation. As data privacy and security concerns grow, governments and regulatory bodies are actively revising and implementing laws to protect PII. The research provides empirical evidence of the need for stringent privacy and security measures, which can inform the development and strengthening of data protection laws and promote the

adoption of new ML technologies within organizations, leading to more robust and effective regulations that protect PII comprehensively.

Finally, this study contributes to the broader conversation on trust-building in cloud applications. Trust is a fundamental factor in online and offline interactions, underpinning relationships between individuals, organizations, and governments. By showcasing the impact that comprehension of PeS and PeP has on the adoption of ML models in cloud environments, this research provides a concrete pathway to building and maintaining trust in the digital age, helping to foster an environment where data can be harnessed for innovation while respecting individuals' rights and privacy.

Recommendations for Action

The results of this study demonstrate that the adoption of ML models in cloud environments can be promoted by improving the perceptions of IT professionals regarding data privacy and data security. Although this finding can be used to promote the implementation of ML models in cloud environments, further actions are needed to enhance and expand data security and data privacy efforts in cloud applications. IT managers should take action to further inform IT professionals about the advantages of ML models through, for example, learning resources used to increase knowledge about data privacy and data security benefits that can be gained through the implementation of ML models in cloud environments.

Based on the findings of this study, IT managers and leaders should consider implementing multiple types of ML models simultaneously, as the use of multiple models can promote a robust security strategy based on multiple security solutions. This

approach helps to provide multiple layers of protection, adapt to evolving threats, and reduce vulnerabilities. IT leaders should comprehensively evaluate available ML security models and consider factors such as effectiveness, scalability, and compatibility with existing systems to determine the most suitable combination for their specific organizational needs.

Additionally, the results of this study help to showcase the significance of policies that promote security and privacy within organizations. Such policies should be based on clear guidelines and emphasize incentives for incorporating ML models into system design and engineering processes. Collaboration between security teams, solutions architects, and senior engineers is crucial for ensuring that ML-based security and privacy considerations are taken into account within the development life cycle. By embedding these practices into the culture and processes of an organization, IT leaders can strengthen their security and privacy efforts and thus create a more trustworthy technological environment.

To further leverage the impact of PeP and PeS on the adoption of ML models in cloud environments, IT managers and leaders should also take action to provide learning resources for their teams. This may include training programs, workshops, and access to educational materials that focus on ML models. Organizations can optimize their security and privacy efforts by equipping their staff with the knowledge and skills to effectively understand and implement these technologies. Moreover, emphasizing the user-friendly nature of some ML models and the tangible benefits of training can boost team confidence in using these tools. IT leaders should work closely with training and

development teams to ensure that these resources align with organizational goals and are readily available to employees at all levels.

Recommendations for Further Research

The main limitation of the study is that the data acquisition was focused specifically on IT project managers and leaders who had three or more years of experience designing and implementing cloud-based applications in organizations and institutions located in South Loop in Chicago, University Park, and Oakbrook. The focus on this target population limits the generalizability of the study, hindering the applicability of the results to different regions or IT sectors. Future studies can be conducted with collection instruments and statistical tools similar to those used in this study to estimate the significance of factors affecting the adoption of ML models in other regions and IT sectors. Furthermore, in this study, the measurement of PeS and PeP was based on subjective assessments of self-perception, which may not fully align with objective perceptions of security and privacy. Future studies can be conducted to evaluate the influence of the implementation of data privacy and data security policies (rather than individuals' perceptions of these policies) on the adoption of multiple types of ML models in cloud environments, and to further investigate which type of ML model is more widely accepted and implemented for specific technological necessities. Future researchers exploring the subject of ML models should consider delving deeper into the algorithms used in these models and their intricate relationship with PeS and PeP. Understanding how specific algorithms impact these perceptions is crucial for refining the design and implementation of ML-based security solutions.

An additional avenue for future investigation is an in-depth analysis of the performance of different ML models in various security contexts. Researchers can examine how different algorithms handle data privacy and data security methods and processes, such as anomaly detection, intrusion prevention, and threat identification. Conducting such investigations can help to determine which algorithms are most effective at enhancing security while preserving privacy, leading to a more informed selection of algorithms for specific security applications. The impact of algorithmic transparency and interpretability on PeS and PeP can also be an essential aspect for examination in future research. Transparency in algorithms can help users understand how security decisions are made, potentially enhancing users' trust in ML models. Researchers examining this subject can delve into the ethical implications of algorithmic choices in ML, considering fairness, bias, and unintended consequences.

Finally, future researchers should develop a comprehensive framework or set of guidelines regarding security and privacy efforts, which will aid in the selection of ML algorithms within organizations. Such guidelines need to account for technical effectiveness and the perceptions of security and privacy, assisting IT managers and leaders in making informed decisions about which algorithms to implement, while considering the potential impact on user trust and confidence. Additionally, exploring the intersection of algorithmic choices, regulatory compliance, and legal requirements is crucial as organizations strive to balance security and privacy with legal obligations. By examining these subjects, researchers can contribute significantly to developing ML

models that are both trusted by users and effective in ensuring data privacy and data security.

Reflections

I had a great learning experience while conducting this study at Walden University. The process of developing a research topic, creating drafts, outlining a prospectus, developing a proposal, performing the research, and writing the study was extremely beneficial for developing my research skills. Having a coherent and clear image of how research methodologies are applied and implemented has expanded my knowledge and furthered my abilities to conduct future research. In addition, I had an eye-opening experience often realizing my chair and committee members were right about questions, modifications, or comments that seemed to conflict with what I had thought to be accurate or correct. This humbling experience taught me that the more I understood the process, the more I realized how little knowledge I had.

One of the most significant challenges I faced was recognizing that my background and experience may have potential effects on the research process. As an individual with a background in IT, I found it necessary to constantly reflect on how my prior knowledge and past professional experiences could influence my research outcomes. It became evident that my enthusiasm for technology could inadvertently shape how I framed my research question, interpreted data, or interacted with study participants. To mitigate this issue, I took deliberate steps to maintain objectivity, such as employing a diverse research team, seeking external input through peer reviews, and

engaging in ongoing self-reflection. By being transparent about my own background and biases, I aimed to minimize any undue influence on the research.

Finally, ethical considerations were paramount for guiding my research. As an IT researcher, I recognized the potential consequences of my work for individuals and organizations. The technology solutions and recommendations I proposed may have far-reaching implications for data security, privacy, and overall well-being. Therefore, it was essential to approach the research with a heightened sense of responsibility, ensuring that the potential benefits outweighed any potential harm. This entailed carefully considering the ethical implications of my research design, data collection methods, and the dissemination of findings. Furthermore, I prioritized data protection and the informed consent of participants to minimize any negative effects on study participants or the broad IT ecosystem.

Summary and Conclusion

Framed on the technology acceptance model (TAM), in this study, quantitative correlational analysis was used to measure data collected from a target population of 106 IT professionals who had three or more years of experience, located in South Loop in Chicago, University Park, and Oakbrook. The purpose of this study was to examine the relationship between IT leaders' comprehension regarding IT project managers' perceived data privacy and perceived data security with the intent to adopt machine learning (ML) models for securing data in cloud-based applications. The data was collected with the use of SurveyMonkey through a self-administered survey based on a 5-point Likert scale. The results of HLR highlighted that two predictors PeP and PeS

explained 53.6% of the variance ($R^2=.536$, $F(8, 97) = 14.006$, $p < .001$). The results indicate that education level ($\beta=-.012$, $p=.895$), leadership roles ($\beta=.141$, $p=.122$), experience at current position ($\beta=-.081$, $p=.292$), and primary cloud computing strategy ($\beta=-.060$, $p=.458$) were not significant predictors. In contrast, experience in cloud computing ($\beta=-.230$, $p=.003$), and industry type ($\beta=.442$, $p=.000$) were significant predictors to the intent to use ML. The relationship between the comprehension of perceptions of data privacy and security with the adoption of ML models can be used by organizations to promote new ML-based technologies that enhance data security and privacy. This will help to build trust and confidence, as well as promote social change by protecting the data of users. As the digital frontier continues to evolve, the findings of this study provide valuable insights into the convergence of ML, cloud security, and the imperative need for addressing the human dimension in the technology adoption efforts aimed at safeguarding and protecting data to ensure the resilience of cloud infrastructures.

References

- Abdelrahman, A. M., Rodrigues, J. J. P. C., Mahmoud, M. M. E., Saleem, K., Das, A. K., Korotaev, V., & Kozlov, S. A. (2021). Software-defined networking security for private data center networks and clouds: Vulnerabilities, attacks, countermeasures, and solutions. *International Journal of Communication Systems*, 34(4). <https://doi.org/10.1002/dac.4706>
- Aburbeian, A. M., Owda, A. Y., & Owda, M. (2022). A technology acceptance model survey of the Metaverse prospects. *AI*, 3(2), 285–302. <https://doi.org/10.3390/ai3020018>
- Adeoye, E., & Osibo, B. (2023). Cloud infrastructure and enterprise IT environment. *International Journal of Latest Technology in Engineering, Management & Applied Science*, 12(09), 22–30. <https://doi.org/10.51583/IJLTEMAS.2023.12903>
- Agresti, A., & Coull, B. A. (1998). “Approximate is better than ‘exact’ for interval estimation of binomial proportions,” *The American Statistician*, 52, 119-126: Comment by Rindskopf and reply. *American Statistician*, 54(1), 88.
- Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, 82(2), 261–277. <https://doi.org/10.1037/h0076477>
- Aldahwan, N. S., & Ramzan, M. S. (2022). The descriptive data analysis for the adoption of community cloud in Saudi HEI-based factor adoption. *BioMed Research International*, 2022, 1–7. <https://doi.org/10.1155/2022/7765204>
- Al-Emran, M., & Granić, A. (2021). Is it still valid or outdated? A bibliometric analysis of the technology acceptance model and its applications from 2010 to 2020. In *AI-*

- Emran, M., Shaalan, K. (Eds.), *Recent advances in technology acceptance models and theories* (Vol. 335, pp. 112). Springer, Cham. https://doi.org/10.1007/978-3-030-64987-6_1
- Alfadda, H. A., & Mahdi, H. S. (2021). Measuring students' use of Zoom application in language course based on the technology acceptance model (TAM). *Journal of Psycholinguistic Research*, 50, 883–900. <https://doi.org/10.1007/s10936-020-09752-1>
- Alghushairy, O., Alsini, R., Soule, T., & Ma, X. (2020). A review of local outlier factor algorithms for outlier detection in big data streams. *Big Data and Cognitive Computing*, 5(1), 1. <https://doi.org/10.3390/bdcc5010001>
- Al Hadwer, A., Tavana, M., Gillis, D., & Rezania, D. (2021). A systematic review of organizational factors impacting cloud-based technology adoption using technology-organization-environment framework. *Internet of Things*, 15, Article 100407. <https://doi.org/10.1016/j.iot.2021.100407>
- Al-Madhagy Taufiq-Hail, G., Rheel A. Alanzi, A., A Mohd Yusof, S., & M Alruwaili, M. (2021). Software as a Service (SaaS) cloud computing: An empirical investigation on university students' perception. *Interdisciplinary Journal of Information, Knowledge, and Management*, 16, 213–253. <https://doi.org/10.28945/4740>
- Alsharif, M., & Rawat, D. B. (2021). Study of machine learning for cloud assisted IoT security as a service. *Sensors*, 21(4), 1034. <https://doi.org/10.3390/s21041034>
- Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. *Qualitative Sociology*, 42(2), 139–160. <https://doi.org/10.1007/s11133-019-9413-7>

- Bloomfield, J., & Fisher, M. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses' Association*, 22(2), 27–30.
<https://doi.org/10.33235/jarna.22.2.27-30>
- Braun, V., Clarke, V., Boulton, E., Davey, L., & McEvoy, C. (2021). The online survey as a qualitative research tool. *International Journal of Social Research Methodology*, 24(6), 641–654. <https://doi.org/10.1080/13645579.2020.1805550>
- Butt, U. A., Mehmood, M., Shah, S. B., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, 9(9), 1379.
<https://doi.org/10.3390/electronics9091379>
- Calver, M., & Fletcher, D. (2020). When ANOVA isn't ideal: Analyzing ordinal data from practical work in biology. *The American Biology Teacher*, 82(5), 289-294.
<https://doi.org/10.1525/abt.2020.82.5.289>
- Chang, Y.-S., Kao, J.-Y., Wang, Y.-Y., & Huang, S.-C. (2021). Effects of cloud-based learning on student's engineering design creativity with different creative self-efficacy. *Thinking Skills and Creativity*, 40, Article 100813.
<https://doi.org/10.1016/j.tsc.2021.100813>
- Changchit, C., & Chuchuen, C. (2018). Cloud computing: An examination of factors impacting users' adoption. *Journal of Computer Information Systems*, 58(1), 1-9.
<https://doi.org/10.1080/08874417.2016.1180651>
- Chauhan, S., Mittal, M., Woźniak, M., Gupta, S., & Pérez de Prado, R. (2021). A technology acceptance model-based analytics for online mobile games using

machine learning techniques. *Symmetry*, 13(8), 1545.

<https://doi.org/10.3390/sym13081545>

Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime detection and prevention efforts in the last decade: An overview of the possibilities of machine learning models. *Review of International Geographical Education Online*, 11(7), 956–974. [10.48047/rigeo.11.07.92](https://doi.org/10.48047/rigeo.11.07.92)

Chkurbene, Z., Abdallah, H. B., Hassine, K., Hamila, R., & Erbad, A. (2021a). Data augmentation for intrusion detection and classification in cloud networks. *2021 International Wireless Communications and Mobile Computing (IWCMC)*.

<https://doi.org/10.1109/iwcmc51323.2021.9498633>

Chkurbene, Z., Erbad, A., Hamila, R., Mohamed, A., Guizani, M., & Hamdi, M. (2020). TIDCS: A dynamic intrusion detection and classification system-based feature selection. *IEEE Access*, 8, 95864-95877.

<https://doi.org/10.1109/access.2020.2994931>

Chkurbene, Z., Hamila, R., Erbad, A., Kiranyaz, S., Al-Emadi, N., & Hamdi, M. (2021b). Cooperative machine learning techniques for cloud intrusion detection. *2021 International Wireless Communications and Mobile Computing (IWCMC)*.

<https://doi.org/10.1109/iwcmc51323.2021.9498809>

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Routledge.

Coker, D. C. (2022). A thematic analysis of the structure of delimitations in the dissertation. *International Journal of Doctoral Studies*, 17, 141-159.

<https://doi.org/10.28945/4939>

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.

<https://doi.org/10.2307/249008>

Disha, R. A., & Waheed, S. (2022). Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique. *Cybersecurity*, 5, Article 1.

<https://doi.org/10.1186/s42400-021-00103-8>

Du, J. (2022). Analysis of a joint data security architecture integrating artificial intelligence and cloud computing in the era of big data. *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* [Conference session], Tirunelveli, India, 988–991.

<https://doi.org/10.1109/icssit53264.2022.9716319>

Dutt, I. (2021). Pre-Processing of KDD'99 & UNSW-NB network intrusion datasets. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(11), 1762-1776. <https://doi.org/10.17762/turcomat.v12i11.6111>

Eddermoug, N., Mansour, A., Sadik, M., Sabir, E., & Azmi, M. (2021). KLM-based profiling and preventing security attacks for cloud computing: A comparative study. *2021 28th International Conference on Telecommunications (ICT)* [Conference session], London, United Kingdom, 1-6.

<https://doi.org/10.1109/ict52184.2021.9511463>

Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of machine learning

- algorithms for anomaly detection. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* [Conference session], Dublin, Ireland, 1-8. <https://doi.org/10.1109/CyberSecurity49315.2020.9138871>
- Ersoy, P. (2021). Evolution of outlier algorithms for anomaly detection. *Manchester Journal of Artificial Intelligence and Applied Sciences*, 2(1).
<https://www.mjaias.co.uk/mj-en/article/view/22>
- Ferri, L., Spanò, R., Maffei, M., & Fiondella, C. (2020). How risk perception influences CEOs' technological decisions: Extending the technology acceptance model to small and medium-sized enterprises' technology decision makers. *European Journal of Innovation Management*, 24(3), 777-798. <https://doi.org/10.1108/ejim-09-2019-0253>
- Fetters, M. D. (2022). A comprehensive taxonomy of research designs, a scaffolded design figure for depicting essential dimensions, and recommendations for achieving design naming conventions in the field of mixed methods research. *Journal of Mixed Methods Research*, 16(4), 394-411.
<https://doi.org/10.1177/15586898221131238>
- Findley, M. G., Kikuta, K., & Denly, M. (2021). External validity. *Annual Review of Political Science*, 24(1), 365-393. <https://doi.org/10.1146/annurev-polisci-041719-102556>
- Fitzpatrick, R., & Stefan, M. I. (2022). Validation through collaboration: Encouraging team efforts to ensure internal and external validity of computational models of biochemical pathways. *Neuroinformatics*, 20, 277-284.

<https://doi.org/10.1007/s12021-022-09584-5>

Frazer, I., Orr, C., & Thielking, M. (2022). Applying the framework method to qualitative psychological research: Methodological overview and worked example. *Qualitative Psychology, 10*(1), 44-59.

<https://doi.org/10.1037/qup0000238>

Greife, M. J., & Maume, M. O. (2020). Stealing like artists: Using court records to conduct quantitative research on corporate environmental crimes. *Journal of Contemporary Criminal Justice, 36*(3), 451-469.

<https://doi.org/10.1177/1043986220931631>

Gupta, D. A., & Gupta, N. (2022). *Research methodology*. SBPD Publications.

https://www.researchgate.net/publication/346492419_Research_Methodology

Hafiz, M. F., Roliana, I., Khairul, A. M., Nashat, A., Ruth, K. C., Mutasem, M. Y., & Omayma, H. A. (2022). A literature review of technology adoption theories and acceptance models for novelty in building information modeling. *Journal of Information Technology Management, 14*, 83–113.

<https://doi.org/10.22059/jitm.2022.84886>

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. *Technology in Society, 67*, Article 101693.

<https://doi.org/10.1016/j.techsoc.2021.101693>

Hatmawan, A. A., & Taufiq, A. R. (2021). Integrating TAM, VAM, PAM and security

- perception in the intention of Fintech service usage. *Journal Management Indonesia*, 21(3), 198. <https://doi.org/10.25124/jmi.v21i3.2650>
- Huang, J., & Li, X. (2022). Ensemble of half-space trees for hyperspectral anomaly detection. *Science China Information Sciences*, 65(9), Article 192103. <https://doi.org/10.1007/s11432-021-3310-x>
- Isautier, J. M., Copp, T., Ayre, J., Cvejic, E., Meyerowitz-Katz, G., Batcup, C., Bonner, C., Dodd, R., Nickel, B., Pickles, K., Cornell, S., Dakin, T., & McCaffery, K. J. (2020). People's experiences and satisfaction with telehealth during the COVID-19 pandemic in Australia: Cross-sectional survey study. *Journal of Medical Internet Research*, 22(12). <https://doi.org/10.2196/24531>
- Ismail, U. M., & Islam, S. (2020). A unified framework for cloud security transparency and audit. *Journal of Information Security and Applications*, 54, Article 102594. <https://doi.org/10.1016/j.jisa.2020.102594>
- Jha, P., & Sharma, A. (2021). Framework to analyze malicious behaviour in cloud environment using machine learning techniques. *2021 International Conference on Computer Communication and Informatics (ICCCI)* [Conference session], Coimbatore, India. <https://doi.org/10.1109/iccci50826.2021.9402671>
- Kalkbrenner, M. T. (2021). A practical guide to instrument development and score validation in the social sciences: The MEASURE Approach. *Practical Assessment, Research, and Evaluation*, 26(1), Article 1. <https://doi.org/10.7275/svg4-e671>
- Kamal, S. A., Shafiq, M., & Kakria, P. (2020). Investigating acceptance of telemedicine

- services through an extended technology acceptance model (TAM). *Technology in Society*, 60, Article 101212. <https://doi.org/10.1016/j.techsoc.2019.101212>
- Kang, H. (2021). Sample size determination and power analysis using the G*Power software. *Journal of Educational Evaluation for Health Professions*, 18, 17. <https://doi.org/10.3352/jeehp.2021.18.17>
- Knief, U., & Forstmeier, W. (2021). Violating the normality assumption may be the lesser of two evils. *Behavior Research Methods*, 53(6), 2576-2590. <https://doi.org/10.3758/s13428-021-01587-5>
- Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing*, 164, 55-68. <https://doi.org/10.1016/j.jpdc.2022.01.030>
- Kyngäs, H. (2020). Qualitative Research and Content Analysis. In H. Kyngäs, K. Mikkonen, & M. Kääriäinen (Eds.), *The Application of Content Analysis in Nursing Science Research*, pp. 3-11. <https://doi.org/10.1007/978-3-030-30199-6>
- Lah, U., Lewis, J. R., & Šumak, B. (2020). Perceived usability and the modified technology acceptance model. *International Journal of Human-Computer Interaction*, 36(13), 1216-1230. <https://doi.org/10.1080/10447318.2020.1727262>
- Lee, W., & Nadim, M. (2020). Kernel-level rootkits features to train learning models against Namespace attacks on containers. *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*

[Conference session], New York, NY, USA. <https://doi.org/10.1109/cscloud-edgecom49738.2020.00018>

- Li, J., Fu, Y., Xu, J., Ren, C., Xiang, X., & Guo, J. (2020). Web application attack detection based on attention and gated convolution networks. *IEEE Access*, 8, 20717-20724. <https://doi.org/10.1109/access.2019.2955674>
- Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy. *ACM Computing Surveys*, 54(2), 1-36. <https://doi.org/10.1145/3436755>
- Lotfaliany, M., Hadaegh, F., Mansournia, M. A., Azizi, F., Oldenburg, B., & Khalili, D. (2022). Performance of stepwise screening methods in identifying individuals at high risk of type 2 diabetes in an Iranian population. *International Journal of Health Policy and Management*, 11(8), 1391-1400. <https://doi.org/10.34172/ijhpm.2021.22>
- Malatji, W. R., Eck, R. V., & Zuva, T. (2020). Understanding the usage, modifications, limitations and criticisms of Technology Acceptance Model (TAM). *Advances in Science, Technology and Engineering Systems Journal*, 5(6), 113-117. <https://doi.org/10.25046/aj050612>
- Mariani, M. M., Ek Styven, M., & Teulon, F. (2021). Explaining the intention to use digital personal data stores: An empirical study. *Technological Forecasting and Social Change*, 166, Article 120657. <https://doi.org/10.1016/j.techfore.2021.120657>
- Mather, M., Hamilton, D., Robalino, S., & Rousseau, N. (2018). Going where other

methods cannot: A systematic mapping review of 25 years of qualitative research in otolaryngology. *Clinical Otolaryngology*, 43(6), 1443-1453.

<https://doi.org/10.1111/coa.13200>

Mayayise, T. (2021). Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption in South Africa. *SA Journal of Information Management*, 23(1). <https://doi.org/10.4102/sajim.v23i1.1376>

Mesfer Alshahrani, H., S. Alsubaei, F., Abdalla Elfadil Eisa, T., K. Nour, M., Ahmed Hamza, M., Motwakel, A., Sarwar Zamani, A., & Yaseen, I. (2022).

Metaheuristics with machine learning enabled information security on cloud environment. *Computers, Materials & Continua*, 73(1), 1557-1570.

<https://doi.org/10.32604/cmc.2022.027135>

Mohammad, A. S., & Pradhan, M. R. (2021). Machine learning with big data analytics for cloud security. *Computers & Electrical Engineering*, 96, Article 107527.

<https://doi.org/10.1016/j.compeleceng.2021.107527>

Moso, J. C., Cormier, S., de Runz, C., Fouchal, H., & Wandeto, J. M. (2021). Anomaly detection on data streams for smart agriculture. *Agriculture*, 11(11), 1083.

<https://doi.org/10.3390/agriculture11111083>

Musyaffi, A. M., & Arinal, M. (2021). Critical factors of cloud accounting acceptance and security for prospective accountants: TAM extension. *Jurnal Riset Akuntansi Kontemporer*, 13(1), 1-6. <https://doi.org/10.23969/jrak.v13i1.3267>

Nadeem, M. A., & Lee, S. U. (2020). Machine learning evaluation of the requirement

- engineering process models for cloud computing and security issues. *Applied Sciences*, 10(17), 5851. <https://doi.org/10.3390/app10175851>
- Nambiar, B. K., & Bolar, K. (2023). Factors influencing customer preference of cardless technology over the card for cash withdrawals: An extended technology acceptance model. *Journal of Financial Services Marketing*, 28(1), 58-73. <https://doi.org/10.1057/s41264-022-00139-y>
- Narayana, G., Pradeepkumar, B., Ramaiah, J. D., Jayasree, T., Yadav, D. L., & Kumar, B. K. (2020). Knowledge, perception, and practices towards COVID-19 pandemic among general public of India: A cross-sectional online survey. *Current medicine research and practice*, 10(4), 153-159. <https://doi.org/10.1016/j.cmrp.2020.07.013>
- Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: A systematic review. *IEEE Access*, 9, 20717-20735. <https://doi.org/10.1109/access.2021.3054129>
- Navaei, M., & Tabrizi, N. (2022). Machine learning in software development life cycle: A comprehensive review. *Proceedings of the 17th International Conference on Evaluation of Novel Approaches to Software Engineering*. <https://doi.org/10.5220/0011040600003176>
- Ntambu, P., & Adeshina, S. A. (2021). Machine learning-based anomalies detection in cloud virtual machine resource usage. *2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS) [Conference session]*, Abuja, Nigeria, 1-6. <https://doi.org/10.1109/icmeas52683.2021.9692308>

- Ntroumpogiannis, A., Giannoulis, M., Myrtakis, N., Christophides, V., Simon, E., & Tsamardinos, I. (2023). A meta-level analysis of online anomaly detectors. *VLDB Journal*, 32(4), 845–886. <https://doi.org/10.1007/s00778-022-00773-x>
- Nyimbili, L., & Chalwe, M. (2023). A review of technology acceptance and adoption models and theories. *International Journal for Multidisciplinary Research (IJFMR)*, 5(6), 1-10. <https://doi.org/10.36948/ijfmr.2023.v05i06.8735>
- Pang, Z., Cen, J., & Yi, M. (2023). Unsupervised concept drift detection method based on Robust Random Cut Forest. *International Journal of Machine Learning and Cybernetics*, 14, 4207–4222. <https://doi.org/10.1007/s13042-023-01890-x>
- Pankowska, M., Pyszny, K., & Strzelecki, A. (2020). Users' adoption of sustainable cloud computing solutions. *Sustainability*, 12(23), Article 9930. <https://doi.org/10.3390/su12239930>
- Pardo, S. (2020). Generalized linear models. *Statistical Analysis of Empirical Data: Methods for Applied Sciences* (pp. 93-106). Springer, Cham. <https://doi.org/10.1007/978-3-030-43328-4>
- Pawar, N. (2020). Type of research and type research design. *Social Research Methodology*, 8(1), 46-57. https://www.researchgate.net/publication/352055750_6_Type_of_Research_and_Type_Research_Design
- Rabe, W., & Kostka, G. (2024). Perceptions of social credit systems in Southeast Asia: An external technology acceptance model. *Global Policy*, 15(2), 314-328. <https://doi.org/10.1111/1758-5899.13337>

- Rafique, H., Almagrabi, A. O., Shamim, A., Anwar, F., & Bashir, A. K. (2020). Investigating the acceptance of mobile library applications with an extended technology acceptance model (TAM). *Computers & Education, 145*, Article 103732. <https://doi.org/10.1016/j.compedu.2019.103732>
- Rahman, A., & Pribadi Subriadi, A. (2022). Software as a Service (SaaS) adoption factors: Individual and organizational perspective. *2022 2nd International Conference on Information Technology and Education (ICIT&E)* [Conference session], Malang, Indonesia, 31–36. <https://doi.org/10.1109/icite54466.2022.9759891>
- Ramesh, J., Sankalpa, D., Aburukba, R., & Elsakhawy, M. (2022). Cloud infrastructure-as-a-Service testbed implementation using OpenStack. *2022 International Symposium on Networks, Computers and Communications (ISNCC)* [Conference session], Shenzhen, China, 1-8. <https://doi.org/10.1109/isncc55209.2022.9851773>
- Razali, N. A., Wan Muhamad, W. N., Ishak, K. K., Saad, N. J., Wook, M., & Ramli, S. (2021). Secure blockchain-based data-sharing model and adoption among intelligence communities. *IAENG International Journal of Computer Science, 48*(1), 18-31. https://www.iaeng.org/IJCS/issues_v48/issue_1/IJCS_48_1_03.pdf
- Sadoughi, F., Ali, O., & Erfannia, L. (2020). Evaluating the factors that influence cloud technology adoption—comparative case analysis of health and non-health sectors: A systematic review. *Health Informatics Journal, 26*(2), 1363-1391. <https://doi.org/10.1177/1460458219879340>
- Sagnier, C., Loup-Escande, E., Lourdeaux, D., Thouvenin, I., & Valléry, G. (2020). User

acceptance of virtual reality: An extended technology acceptance model.

International Journal of Human-Computer Interaction, 36(11), 993-1007.

<https://doi.org/10.1080/10447318.2019.1708612>

Sana, M. U., Li, Z., Javaid, F., Liaqat, H. B., & Ali, M. U. (2021). Enhanced security in cloud computing using neural network and encryption. *IEEE Access*, 9, 145785-

145799. <https://doi.org/10.1109/access.2021.3122938>

Sauber, A. M., El-Kafrawy, P. M., Shawish, A. F., Amin, M. A., & Hagag, I. M. (2021).

A new secure model for data protection over cloud computing. *Computational*

Intelligence and Neuroscience, 2021, 1-11. <https://doi.org/10.1155/2021/8113253>

Shyam, G. K., & Doddi, S. (2019). Achieving cloud security solutions through machine and non-machine learning techniques: A Survey. *Journal of Engineering Science & Technology Review*, 12(3), 51-63.

<http://jestr.org/downloads/Volume12Issue3/fulltext81232019.pdf>

Siagian, H., Tarigan, Z. J., Basana, S. R., & Basuki, R. (2022). The effect of perceived security, perceived ease of use, and perceived usefulness on consumer behavioral intention through trust in digital payment platform. *International Journal of Data and Network Science*, 6(3), 861-874. <https://doi.org/10.5267/j.ijdns.2022.2.010>

Skafi, M., Yunis, M. M., & Zekri, A. (2020). Factors influencing SMEs' adoption of cloud computing services in Lebanon: An empirical analysis using TOE and contextual theory. *IEEE Access*, 8, 79169-79181.

<https://doi.org/10.1109/access.2020.2987331>

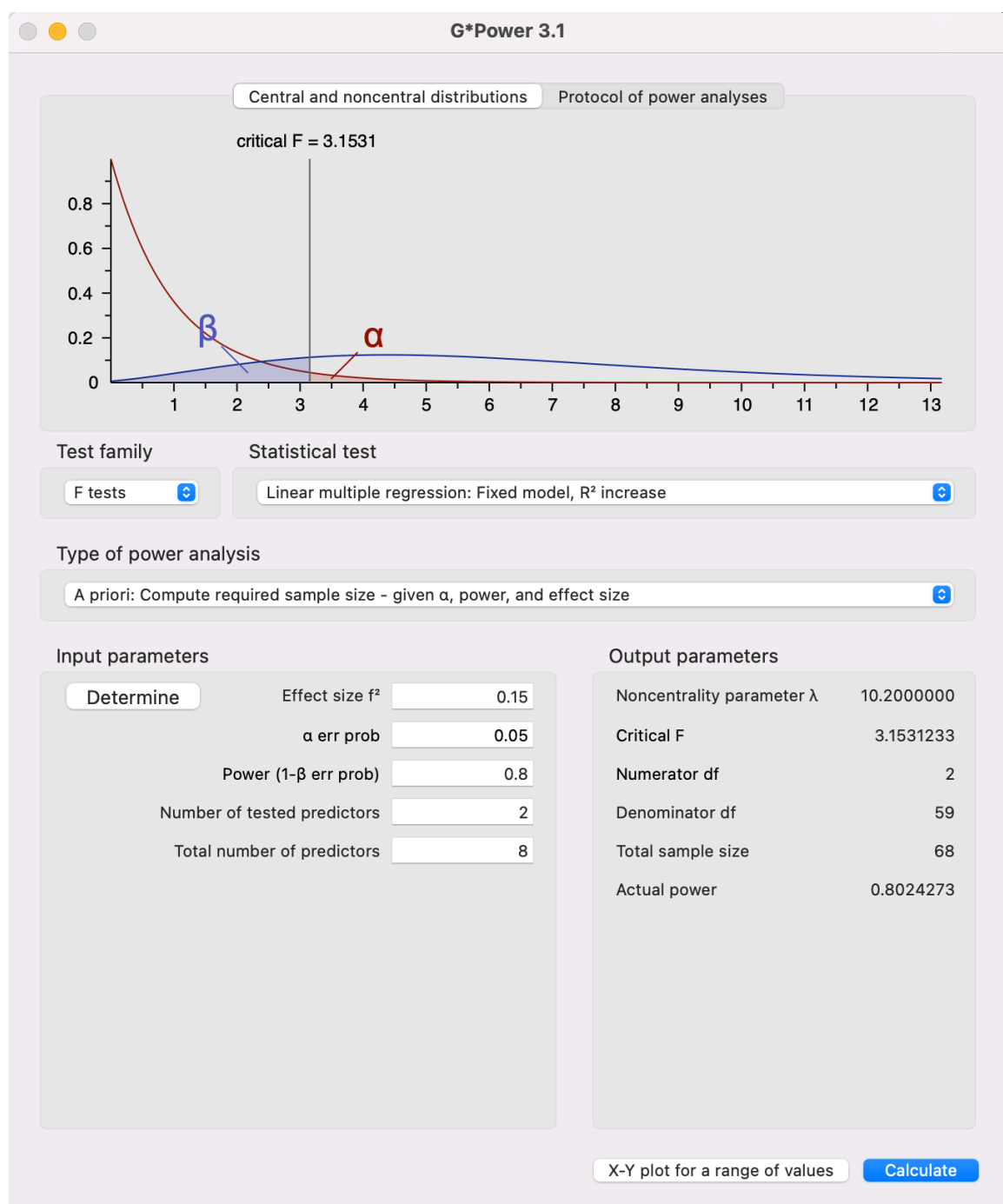
Staerman, G., Adjakossa, E., Mozharovskyi, P., Hofer, V., Sen Gupta, J., & Cl emen on,

- S. (2022). Functional anomaly detection: A benchmark study. *International Journal of Data Science and Analytics*, 16(1), 101-117.
<https://doi.org/10.1007/s41060-022-00366-5>
- Stieninger, M., Nedbal, D., Wetzlinger, W., Wagner, G., & Erskine, M. A. (2022). Factors influencing the organizational adoption of cloud computing: A survey among cloud workers. *International Journal of Information Systems and Project Management*, 6(1), 5-23. <https://doi.org/10.12821/ijispm060101>
- Tella, A., Ukwoma, S. C., & Kayode, A. I. (2020). A two models modification for determining cloud computing adoption for web-based services in academic libraries in Nigeria. *The Journal of Academic Librarianship*, 46(6), Article 102255. <https://doi.org/10.1016/j.acalib.2020.102255>
- Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, 7(2), 69-84.
<https://doi.org/10.1007/s40860-020-00115-0>
- Tiwari, P. K., Kannan, K., Veeraiah, D., Ranjan, N., Singh, J., Alshammri, G. H., & Halifa, A. (2022). Security protection mechanism in cloud computing authorization model using machine learning techniques. *Wireless Communications and Mobile Computing*, 2022, 1-12.
<https://doi.org/10.1155/2022/1907511>
- Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The Processes of Technological Innovation*. Lexington Books.

- Tripathy, D., Gohil, R., & Halabi, T. (2020). Detecting SQL injection attacks in cloud SaaS using machine learning. *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)* [Conference session], Baltimore, MD, USA, 145–150.
<https://doi.org/10.1109/bigdatasecurity-hpsc-ids49724.2020.00035>
- Vahdat, A., Alizadeh, A., Quach, S., & Hamelin, N. (2021). Would you like to shop via mobile app technology? The technology acceptance model, social factors and purchase intention. *Australasian Marketing Journal*, 29(2), 187-197.
<https://doi.org/10.1016/j.ausmj.2020.01.002>
- Varghese, M., & Jose, M. V. (2021). Securing cloud from attacks: Machine learning based intrusion detection in cloud sensor networks. *Adhoc & Sensor Wireless Networks*, 50(1-4), 143–171. <https://www.oldcitypublishing.com/journals/ahswn-home/ahswn-issue-contents/ahswn-volume-50-number-1-4-2021/20233-2/>
- Veloso, C. M., Sousa, B., Au-Yong-Oliveira, M., & Walter, C. E. (2021). Boosters of satisfaction, performance and employee loyalty: Application to a recruitment and outsourcing information technology organization. *Journal of Organizational Change Management*, 34(5), 1036-1046. <https://doi.org/10.1108/jocm-01-2021-0015>
- Walters, W. H. (2021). Survey design, sampling, and significance testing: Key issues. *The Journal of Academic Librarianship*, 47(3), Article 102344.
<https://doi.org/10.1016/j.acalib.2021.102344>

- Wang, H. B., & Gao, Y. J. (2021). Research on C4. 5 algorithm improvement strategy based on MapReduce. *Procedia Computer Science*, 183, 160-165.
<https://doi.org/10.1016/j.procs.2021.02.045>
- Webb, J., & Aly, O. (2020). Relationship between acceptance of virtual private cloud (VPC) and adoption of VPC: An empirical study. *IUP Journal of Information Technology*, 16(1), 19–76.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3798217
- Weng, F., Yang, R., Ho, H., & Su, H. (2021). A TAM-based study of the attitude towards use intention of multimedia among school teachers. *Applied System Innovation*, 1(3), 36. <https://doi.org/10.3390/asi1030036>
- Yussupov, V., Soldani, J., Breitenbücher, U., Brogi, A., & Leymann, F. (2021). FaaSten your decisions: A classification framework and technology review of function-as-a-Service platforms. *Journal of Systems and Software*, 175, Article 110906.
<https://doi.org/10.1016/j.jss.2021.110906>

Appendix A: G*Power Analysis to Determine Sample Size



Appendix B: Invitation

My Name is Ali Sanad, and I am doctoral candidate in the Doctor of Information Technology program at Walden University. I am honored to invite you to participate in a survey for my study titled *The Impact of Machine Learning Security Models on Cloud Data Security*.

Eligibility Requirements:

- You are a manager, project manager, leader, and/or architect in your organization's information technology department.
- You manage, lead, architect, or oversee applications within cloud infrastructure.
- You have more than one (1) year of exposure to cloud infrastructure.
- You have more than eight (8) years of overall work experience in computer science or any related field.
- Your organization and/or company has been subscribed to cloud computing services for more than two (2) years.
- Your application deals with security requirements that emphasize data security and data privacy.
- You are over the age of 18.

Survey Link:

The survey can be found Survey Monkey with the link: <Link>

Contact or Questions:

If you have any questions, please contact me at 630-754-9600 or ali.sanad@waldenu.edu.
Ali Sanad

Appendix C: Aburbeian et al. (2022) Permission to Use

[↩ Reply](#)
[↩ Reply all](#)
[→ Forward](#)
[📁 Archive](#)
[🗑️](#)

Re:


Amani Yousef Issa Owda <Amani.Owda@aaup.edu>
 3:00 AM

To: Ali Sanad Cc: "Alsharif Hasan" Mohamad Abed Abu Rbeian; Majdi Sabe Mofadi Owda

Dear Ali,

Thanks for your email. Yes you can reuse it subject to make a reference for the paper.

Dr Majdi and Alsharif Hassan are copied in the email.

Kind Regards

Amani

Dr. Amani Owda, BEng, MSc, PGC AP, UK-FHEA, Ph.D.
 Assistant Professor in Computer Engineering
 Head of Department of Natural, Engineering, and Technology Sciences
 Faculty of Graduate Studies

Arab American University - Palestine
 AAUP Campus, Dahyat Alrehan, Ramallah, West Bank, Palestine, P622
 Email: Amani.Owda@aaup.edu

AAUP Website:

<https://www.aaup.edu/amani.owda>

Google Scholar Website:

<https://scholar.google.com/citations?user=0Ccydi8AAAAJ&hl=en>

ResearchGate Website:

<https://www.researchgate.net/profile/Amani-Owda>



From: Ali Sanad <ali.sanad@walden.edu>
Sent: 21 December 2022 03:18
To: Amani Yousef Issa Owda <Amani.Owda@aaup.edu>
Subject:

Hello Dr. Owda,

I hope this email finds you well. My name is Ali Sanad, and I am a doctoral student at the Walden University Doctor of Information Technology (DIT) program. I am currently working on developing a survey design for my study and I am seeking your permission to utilize and use your survey instruments in the published Article "A Technology Acceptance Model Survey of the Metaverse Prospects" in the MDPI journal. The focus of my study is to examine the relationship between IT project managers' perceived security and perceived privacy with the intent to use ML security models for securing cloud-based applications' data. The theory that will ground this study include Davis (1989) technology acceptance model (TAM).

I would greatly appreciate your approval to use and modify your survey and I look forward to hearing from you soon.

Sent from [Mail](#) for Windows

Appendix D: Instrument Used to Collect Data

No.	Question	Value	Scale
1.	Are you a project manager, manager, or a leader in your organization's IT department?	(1) Yes (2) No	Nominal
2.	Does your project, solution, resources, or services reside in the cloud?	(1) Yes (2) No	Nominal
3.	Has your organization been subscribed to cloud services for more than one (1) year?	(1) Yes (2) No	Nominal
4.	What is your highest education level?	(1) Less than high school (2) High school/GED (3) Some College (4) Associates (5) Bachelor's degree (6) Master's degree (7) PhD/Doctorate	Nominal
5.	What is your project management, management, or project role in your current position?	(1) Tech Lead (2) Principal (3) Architect (4) Project Manager (5) Directing Manager (6) Executing manager	Nominal
6.	How long have you been in your current position?	(1) Less than 1 year (2) 1 to 3 years (3) 3 to 5 years (4) More than 5 years	Nominal
7.	How many years of experience do you have in cloud computing?	(1) Less than 1 year (2) 1 to 3 years (3) 3 to 5 years (4) More than 5 years	Nominal
8.	How many employees are in your company?	(1) Less than 100 employees (2) 100 to 500 employees (3) 500 to 1000 employees (4) More than 1000 employees	Nominal

9.	What is your project's cloud computing model strategy?	(1) IaaS (2) SaaS (3) PaaS (4) Hybrid	Nominal
10.	What is your project's primary cloud deployment model strategy? Nominal	(1) Community Cloud (2) Public Cloud (3) Private Cloud (4) Hybrid	Nominal
11.	What is your company's industry type or primary business?	(1) Agriculture, Forestry, & Wildlife (2) Automotive, Sales, & Marketing (3) Cloud Service Provider & IT Services (4) Construction, Real Estate, & Housing (5) Education (6) Energy, Utilities, & Gas (7) Financial, Insurance, Banking, & Legal (8) Food & Hospitality (9) Government & Military (10) Health Care & Pharmaceutical (11) Non-profit (12) Other	Nominal
	Perceived Usefulness		
12.	Using the ML security models helps me control cloud-based apps security.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
13.	Using the ML security models in my cloud-based apps enhances security performance.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
14.	I find the ML security models useful in my cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither	Ordinal

		(4) Agree (5) Strongly agree	
15.	Using ML security models makes it easier to enhance cloud-based apps security control.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
16.	Using ML security models would increase productivity.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
	Perceived Ease of Use		
17.	Learning to implement ML security models would be easy for me	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
18.	It is easy to become skillful at using ML security models.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
19.	I find it easy to apply the ML security models for my application.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
20.	Using ML security models is easy and understandable.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
21.	Using ML security models is flexible to implement compared to non-ML approaches.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
	Attitude Toward Using		
22.	Using ML security models is good.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal

23.	My using ML security models for securing cloud-based applications is favorable.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
24.	It is a positive influence for me to use ML security models in my cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
25.	I think it is valuable to use ML security models in cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
26.	I think it is a trend to use ML security models in cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
	Intention to Use	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
27.	I tend to use ML security models in my cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
28.	I increase the occurrences of using ML security models in my cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
29.	Using ML security models in my cloud-based app to enhance security.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
30.	I'd love to use ML security models in my cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither	Ordinal

		(4) Agree (5) Strongly agree	
31.	I use ML security models to provide elevated security to my cloud-based apps.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
	Perceived Privacy		
32.	Using the ML security models helps me increase data privacy.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
33.	Using the ML security models enhances data privacy measures.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
34.	I find the ML security models useful in my data privacy.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
35.	Using ML security models makes it easier to enhance data privacy control.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
	Perceived Security		
36.	Using the ML security models helps me increase data security.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
37.	Using the ML security models enhances data security measures.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
38.	I find the ML security models useful in my data security.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal

39.	Using ML security models makes it easier to enhance data security control.	(1) Strongly disagree (2) Disagree (3) Neither (4) Agree (5) Strongly agree	Ordinal
ML Security Model Implemented			
40.	Have you or your organization implemented ML security models for any cloud-based applications? If No, select none.	(1) Anomaly Detection Models (2) Intrusion Detection and Prevention Systems (IDPS) (3) Malware Detection Models (4) User Behavior Analytics (UBA) (5) Security Information and Event Management (SIEM) (6) Data Loss Prevention (DLP) (7) Access Control Models (8) Threat Intelligence Models (9) Encryption and Cryptography Models (10) Adversarial Machine Learning (AML) (11) Other (12) None	Nominal