Intelligent Information Management, 2024, 16, 176-193
https://www.scirp.org/journal/iim
ISSN Online: 2160-5920
ISSN Print: 2160-5912

Enhancing Cybersecurity through Cloud Computing Solutions in the United States

Omolola F. Hassan[1], Folorunsho O. Fatai[1], Oluwadare Aderibigbe[1], Abdullah Oladoyin Akinde[1], Tolulope Onasanya[2], Mariam Adetoun Sanusi[3], Oduwunmi Odukoya[4]

[1]Department of Computer Science, Austin Peay State University, Clarksville, USA
[2]Department of Computer Science, North Carolina Agricultural and Technical State University, Greensboro, USA
[3]Department of Cybersecurity, University of Texas, Dallas, USA
[4]Department of Information Systems, East Tennessee State University, Johnson City, USA
Email: omololafeyikemi@gmail.com, ffolorunsho@my.apsu.edu, oaderibigbe@my.apsu.edu, akinde.abdullah@gmail.com, tdonasanya@aggies.ncat.edu, sanusiadetoun@gmail.com, odukoyao@etsu.edu

How to cite this paper: Hassan, O.F., Fatai, F.O., Aderibigbe, O., Akinde, A.O., Onasanya, T., Sanusi, M.A. and Odukoya, O. (2024) Enhancing Cybersecurity through Cloud Computing Solutions in the United States. *Intelligent Information Management*, **16**, 176-193.
https://doi.org/10.4236/iim.2024.164011

Received: May 23, 2024
Accepted: July 9, 2024
Published: July 12, 2024

Abstract

This study investigates how cybersecurity can be enhanced through cloud computing solutions in the United States. The motive for this study is due to the rampant loss of data, breaches, and unauthorized access of internet criminals in the United States. The study adopted a survey research design, collecting data from 890 cloud professionals with relevant knowledge of cybersecurity and cloud computing. A machine learning approach was adopted, specifically a random forest classifier, an ensemble, and a decision tree model. Out of the features in the data, ten important features were selected using random forest feature importance, which helps to achieve the objective of the study. The study's purpose is to enable organizations to develop suitable techniques to prevent cybercrime using random forest predictions as they relate to cloud services in the United States. The effectiveness of the models used is evaluated by utilizing validation matrices that include recall values, accuracy, and precision, in addition to F1 scores and confusion matrices. Based on evaluation scores (accuracy, precision, recall, and F1 scores) of 81.9%, 82.6%, and 82.1%, the results demonstrated the effectiveness of the random forest model. It showed the importance of machine learning algorithms in preventing cybercrime and boosting security in the cloud environment. It recommends that other machine learning models be adopted to see how to improve cybersecurity through cloud computing.

Keywords

Cybersecurity, Cloud Computing, Cloud Solutions, Machine Learning, Algorithm

1. Introduction

In today's fast-changing digital ecosystem, cybersecurity concerns have become more sophisticated and ubiquitous, posing substantial dangers to individuals, corporations, and governments worldwide [1] [2]. The proliferation of networked devices, the exponential expansion of data, and the advent of sophisticated cyber threats have highlighted the crucial role of cybersecurity in protecting sensitive information and guaranteeing the integrity of digital systems [3]. However, one of the most significant issues in cybersecurity today is the sheer amount and diversity of cyber-attacks. Cybercriminals constantly devise new strategies and ways to exploit software, networks, and human behavioral flaws. From malware and phishing assaults to ransomware and data breaches, cyber dangers are diverse and ever-changing. These attacks can have disastrous repercussions, ranging from financial losses and reputational harm to interruption of essential services and national security concerns [3]. In 2023 alone, [4] reported losses exceeding $4.2 billion due to cybercrime, with businesses of all sizes being targeted. The scale of these crimes ranges from small-scale phishing attempts aimed at individual employees to sophisticated, large-scale breaches that can compromise the personal data of millions of customers. The impact on organizations is profound, leading to financial losses, reputational damage, legal repercussions, and disruptions in operations. For instance, the average cost of a data breach in the U.S. is estimated to be $8.64 million, significantly higher than the global average [4] [5].

Furthermore, another critical concern is the increased interconnection of digital ecosystems. The attack surface has grown tremendously as cloud computing, Internet of Things (IoT) devices, and networked networks have become more commonplace. Cybercriminals can use flaws in any networked device or system to obtain unauthorized access, modify data, or execute distributed denial-of-service (DDoS) assaults. The linked nature of digital systems increases the potential impact of cyber-attacks, making it more challenging to prevent and mitigate their effects [6] [7]. Furthermore, the increased digitalization of vital infrastructure and essential services has generated new cybersecurity threats. Healthcare, banking, energy, and transportation industries rely extensively on digital technology to supply services and manage operations [8]. However, integrating digital technologies into critical infrastructure exposes them to various cyber risks, including targeted assaults on industrial control systems and supply chain intrusions. A positive cyber-attack on critical infrastructure can have far-reaching implications, interrupting vital services, inflicting extensive economic harm, and endangering public safety [6] [7] [8].

Moreover, the human component remains a significant cybersecurity concern. Despite technological and security breakthroughs, cyber attackers exploit human mistakes and neglect [7]. Phishing attacks, social engineering strategies, and insider threats use human weaknesses to obtain unauthorized access to systems or sensitive data. Inadequate cybersecurity knowledge and employee training

heighten the likelihood of human-related security events, emphasizing the necessity of fostering a cybersecurity awareness and vigilance culture inside organisations [6]. Furthermore, it is observed that geopolitical conflicts and state-sponsored cyber operations are becoming more prevalent in the global cybersecurity scene. Nation-state actors use cyber espionage, sabotage, and warfare to accomplish political, economic, or military goals [8]. Sophisticated cyber-attacks ascribed to nation-states frequently target government institutions, defense contractors, critical infrastructure, and multinational firms, providing considerable difficulties for cybersecurity practitioners and policymakers alike [9].

Furthermore, cybersecurity threats in today's digital ecosystem are multidimensional and ever-changing, influenced by technological breakthroughs, interconnection, human behavior, and geopolitical dynamics. Addressing these difficulties necessitates a comprehensive and adaptable strategy that includes technology solutions, strong cybersecurity legislation and regulations, cybersecurity awareness and education campaigns, and international collaboration [10]. Cybersecurity will remain a top priority as the digital ecosystem evolves, necessitating continuous innovation and collaboration to reduce cyber-attacks and protect the integrity of digital systems and information [11].

Additionally, in recent years, cloud computing has emerged as a significant tool for addressing cybersecurity concerns in the digital environment. The advent of cloud computing has changed how computer resources are delivered, accessed, and managed, with considerable security, scalability, and flexibility benefits [9]. It should also be mentioned that, at its heart, cloud computing refers to the distribution of computing services through the Internet, allowing users to access a shared pool of resources on demand, such as servers, storage, networking, and applications. Cloud computing users can pay for the infrastructure and services provided by cloud service providers (CSPs) [10], in contrast to traditional on-premises infrastructure, which necessitates businesses to purchase and maintain their gear and software.

However, one of the primary benefits of cloud computing in terms of cybersecurity is the increased security measures provided by credible CSPs. Leading cloud providers spend extensively on cutting-edge security technology, infrastructure, and experience to safeguard their cloud environments from cyber-attacks. These security measures include strong encryption, Identity and Access Management (IAM), network segmentation, intrusion detection and prevention systems (IDPS), and frequent security audits and assessments [12]. Furthermore, by using cloud providers' security capabilities, organizations may improve their cybersecurity posture without incurring significant upfront costs for security equipment and knowledge. This is especially useful for small and medium-sized enterprises (SMBs), who may need more capacity to adopt complete cybersecurity measures on their own [13] [14].

Furthermore, cloud computing provides inherent scalability and flexibility, allowing organizations to quickly scale their computer resources up or down in

response to demand. This agility enables organizations to adapt swiftly to cybersecurity risks and needs, such as unexpected traffic surges or implementing extra security measures in response to emerging threats [15]. Cloud computing also allows centralized management and control of security policies and configurations across several environments. Organizations may obtain insight into their cloud infrastructure, monitor security incidents in real time, and enforce uniform security rules and controls across their cloud footprint using centralized dashboards and management interfaces [16].

Furthermore, cloud computing allows organizations to use advanced security services and technologies that would be prohibitively expensive or difficult to install on-premises. These include cloud-based security analytics and machine learning algorithms for threat detection and response, automated security orchestration and remediation tools, and cloud-based backup and disaster recovery systems [12]. However, [15] noted that while cloud computing has various benefits for cybersecurity, it has risks and considerations. Organizations must carefully address the security consequences of transferring sensitive data and workloads to the cloud, such as data privacy and compliance obligations, regulatory concerns, and the shared responsibility model for cloud security.

Additionally, organizations must have robust cloud security governance frameworks to manage risks and compliance needs in the cloud efficiently. This involves developing clear security policies and processes, conducting frequent security assessments and audits, and offering continuing cybersecurity training and awareness programs to staff [14]. Furthermore, cloud computing is a tempting solution to cybersecurity challenges in the digital era, providing superior security, scalability, flexibility, and cost-effectiveness compared to traditional on-premises infrastructure. Organizations may improve their cybersecurity posture and defend their digital assets from growing cyber threats by exploiting cloud computing's security capabilities and benefits. However, successful cloud computing adoption necessitates careful planning, governance, and continual monitoring to ensure that security risks are appropriately managed and mitigated [13]. However, the study aims to improve cybersecurity by implementing cloud computing technologies to meet cybersecurity concerns.

2. Literature Review

The confidentiality, integrity, and availability of digital assets and systems are in danger from a wide range of harmful behaviors and vulnerabilities that fall under cybersecurity threats and vulnerabilities [14]. Malware, which includes viruses, worms, Trojan horses, ransomware, and spyware, is a common danger to cybersecurity. Its goal is to compromise computers, steal confidential data, or interfere with regular business processes. Phishing attacks refer to deceptive emails, messages, or websites that fool users into downloading dangerous software or disclosing personal information [14]. Attacks are known as denial-of-service (DoS) and distributed denial-of-service (DDoS) overload systems

or networks with excessive traffic, making them unavailable to authorized users. Insider threats refer to the evil or careless acts of workers, subcontractors, or reliable persons accessing confidential information or systems [14].

2.1. Cloud Computing and Its Relevance to Cybersecurity

Cloud computing has completely changed how organizations manage and deliver computing services, offering a scalable, on-demand model for accessing shared resources over the Internet. At its core, cloud computing allows users to leverage a pool of computing resources, including servers, storage, networking, and applications, without upfront investment in hardware or infrastructure. Instead, users can access these resources on a pay-as-you-go basis, scaling up or down based on demand [16]. Furthermore, the relevance of cloud computing to cybersecurity rests in its ability to address critical challenges and enhance security posture in the digital age [17] [18] noted that one of the primary advantages of cloud computing is the robust security measures offered by reputable cloud service providers (CSPs). Leading CSPs invest heavily in state-of-the-art security technologies, infrastructure, and expertise to protect their cloud environments from cyber threats. These security measures include encryption, Identity and Access Management (IAM), network segmentation, intrusion detection and prevention systems (IDPS), and regular security audits and assessments [17].

Additionally, by leveraging the security capabilities of cloud providers, organizations can strengthen their cybersecurity posture without the need for significant upfront investment in security infrastructure and expertise. This is particularly beneficial for small and medium-sized businesses (SMBs) that may need more resources to implement comprehensive cybersecurity measures on their own [13] [19]. Furthermore, cloud computing offers inherent scalability and flexibility, enabling organizations to rapidly scale their computing resources up or down based on demand. The agility allows organizations to quickly respond to changing cybersecurity threats and requirements, such as sudden spikes in traffic or the need to deploy additional security controls in response to emerging threats [20].

Also, cloud computing facilitates centralized management and control of security policies and configurations across distributed environments. Through centralized dashboards and management consoles, organizations can gain visibility into their cloud infrastructure, monitor real-time security events, and enforce consistent security policies and controls across their entire cloud footprint [17]. Moreover, cloud computing enables organizations to leverage advanced security services and technologies that may be prohibitively expensive or complex to implement on-premises. These include cloud-based security analytics and machine learning algorithms for threat detection and response, automated security orchestration and remediation tools, and cloud-based backup and disaster recovery solutions [19] [20].

However, [19] noted that while cloud computing offers numerous cybersecur-

ity benefits, it has challenges and considerations. Organizations must carefully assess the security implications of migrating sensitive data and workloads to the cloud, including data privacy and compliance requirements, regulatory considerations, and the shared responsibility model for cloud security. Cloud computing represents a compelling solution to cybersecurity issues in the digital age, offering enhanced security, scalability, flexibility, and cost-effectiveness compared to traditional on-premises infrastructure. By leveraging the security capabilities and advantages of cloud computing, organizations can strengthen their cybersecurity posture and better protect their digital assets against evolving cyber threats [19]. However, [18] noted that the successful adoption of cloud computing requires careful planning, governance, and ongoing vigilance to ensure that security risks are effectively managed and mitigated.

2.2. Benefits of Cloud Computing for Cybersecurity

Cloud computing offers numerous benefits for cybersecurity, providing organizations with enhanced security measures, scalability, flexibility, and cost-effectiveness compared to traditional on-premises infrastructure [21] [22] noted that one of the primary advantages of cloud computing is the robust security measures offered by reputable cloud service providers (CSPs). Leading CSPs invest heavily in state-of-the-art security technologies, infrastructure, and expertise to protect their cloud environments from cyber threats. These security measures include encryption, Identity and Access Management (IAM), network segmentation, intrusion detection and prevention systems (IDPS), and regular security audits and assessments. However, [23] stated that by leveraging the security capabilities of cloud providers, organizations can strengthen their cybersecurity posture without the need for significant upfront investment in security infrastructure and expertise.

Furthermore, cloud computing offers inherent scalability and flexibility, enabling organizations to rapidly scale their computing resources up or down based on demand. This agility allows organizations to quickly respond to changing cybersecurity threats and requirements, such as sudden spikes in traffic or the need to deploy additional security controls in response to emerging threats. The ability to scale resources dynamically ensures that organizations can maintain optimal performance and resilience in the face of evolving cyber threats [22]. Cloud computing also facilitates centralized management and control of security policies and configurations across distributed environments. Through centralized dashboards and management consoles, organizations can gain visibility into their cloud infrastructure, monitor real-time security events, and enforce consistent security policies and controls across their entire cloud footprint. This centralized approach to security management helps organizations streamline security operations, reduce complexity, and improve overall governance and compliance [21].

Moreover, cloud computing enables organizations to leverage advanced secu-

rity services and technologies that may be prohibitively expensive or complex to implement on-premises. These include cloud-based security analytics and machine learning algorithms for threat detection and response, automated security orchestration and remediation tools, and cloud-based backup and disaster recovery solutions. By harnessing these advanced security capabilities, organizations can enhance their ability to detect, mitigate, and recover from cyber threats more effectively and efficiently [23]. Overall, cloud computing offers significant benefits for cybersecurity, providing organizations with enhanced security measures, scalability, flexibility, and cost-effectiveness compared to traditional on-premises infrastructure. By leveraging the security capabilities and advantages of cloud computing, organizations can strengthen their cybersecurity posture, improve resilience to cyber threats, and better protect their digital assets against evolving security risks. However, the successful adoption of cloud computing requires careful planning, governance, and ongoing vigilance to ensure that security risks are effectively managed and mitigated [21].

2.3. Practices for Implementing Cloud-Based Cybersecurity Solutions

Implementing cloud-based cybersecurity solutions requires a comprehensive approach encompassing strategic planning, robust security controls, continuous monitoring, and adherence to industry best practices [24]. By following these practices, organizations can effectively implement cloud-based cybersecurity solutions to protect their assets, data, and operations in the cloud. By prioritizing security, adhering to best practices, and continuously monitoring and improving security posture, organizations can enhance the resilience of their cloud deployments and mitigate the risk of cyber threats and vulnerabilities [25] [26]. Here are several critical practices to consider when implementing cloud-based cybersecurity solutions:

- Risk Assessment and Management: Conduct a thorough risk assessment to identify potential security threats, vulnerabilities, and compliance requirements associated with cloud deployments. Develop a risk management plan that outlines strategies for mitigating identified risks and prioritizes security measures based on their impact and likelihood of occurrence [25].
- Security by Design: Implement a security-by-design approach when architecting cloud infrastructure and applications. Incorporate security controls and best practices into the design phase, including encryption, access controls, network segmentation, and secure coding principles. By building security into cloud environments from the outset, organizations can reduce the risk of security breaches and vulnerabilities [25].
- Identity and Access Management (IAM): Implement robust IAM controls to manage user identities, access permissions, and authentication mechanisms in cloud environments. Utilize centralized identity management systems, multi-factor authentication (MFA), and role-based access controls (RBAC) to

enforce least privilege access and mitigate the risk of unauthorized access to sensitive data and resources [26].

- Data Encryption: Encrypt data both in transit and at rest to protect it from unauthorized access and interception. Utilize encryption protocols and algorithms to secure data transmissions between users and cloud services and encryption mechanisms to safeguard data stored in cloud storage repositories. Implement critical management practices to securely manage encryption keys and ensure the integrity and confidentiality of encrypted data [25].
- Security Monitoring and Incident Response: Implement robust security monitoring and incident response capabilities to detect, respond to, and mitigate security incidents in cloud environments. Utilize security information and event management (SIEM) systems, intrusion detection and prevention systems (IDPS), and cloud-native monitoring tools to monitor suspicious activities, anomalies, and potential security breaches. Develop and test incident response plans to ensure timely and effective response to security incidents and minimize their impact on cloud operations [25].
- Regular Security Audits and Assessments: Conduct regular security audits and assessments of cloud environments to evaluate compliance with security policies, regulatory requirements, and industry standards. Utilize third-party security assessment services, penetration testing, and vulnerability scanning tools to identify security weaknesses and gaps in cloud configurations. Implement remediation measures and continuous improvement initiatives based on audit findings to enhance the security posture of cloud deployments [27].

2.4. Challenges and Risks Associated with Third-Party Cloud Service Providers

Third-party cloud service providers offer numerous benefits, including scalability, flexibility, and cost-effectiveness. However, entrusting sensitive data and critical operations to external providers also introduces several challenges and risks that organizations must address to ensure the security and integrity of their cloud environments [6]. However, one of the primary challenges associated with third-party cloud service providers is losing control over data and infrastructure. When organizations migrate their data and workloads to the cloud, they rely on the provider to manage and secure their assets effectively. However, relinquishing direct control over infrastructure and security measures can introduce uncertainty and potential vulnerabilities, as organizations may need complete visibility or transparency into the provider's practices and procedures [26].

Additionally, the shared responsibility model for cloud security complicates the allocation of security responsibilities between the organization and the cloud service provider. While the provider is responsible for securing the underlying infrastructure and platform, organizations are typically responsible for securing their applications, data, and access controls. This division of responsibilities can

lead to confusion or gaps in security coverage, particularly if organizations fail to implement adequate security measures on their end [6]. Furthermore, the multi-tenant nature of cloud environments introduces the risk of data exposure or leakage due to inadequate isolation between tenants. Shared resources, such as servers, storage, and networking infrastructure, increase the potential for unauthorized access or data breaches if proper isolation controls are not in place. Organizations must carefully assess the provider's isolation mechanisms and security controls to mitigate the risk of data exposure in multi-tenant environments [27].

Furthermore, another difficulty is the possibility of service outages or interruptions because of hardware failures, software flaws, cyber assaults, or natural catastrophes impacting the provider's network. While credible cloud providers invest in redundant infrastructure and disaster recovery methods to reduce downtime, organizations must still prepare for any interruptions and create backup and contingency plans to maintain business continuity [9]. Concerns about data privacy, compliance, and legal obligations can also present substantial issues when committing data to third-party cloud providers. Organizations must verify that their data handling processes comply with applicable rules, such as GDPR, HIPAA, and PCI DSS, and that the supplier provides enough guarantees and compliance certifications to satisfy their legal and regulatory requirements [15].

To effectively address these issues, however, organizations must take a proactive approach to cloud security. This includes choosing cloud providers with great care, negotiating detailed service level agreements (SLAs), putting strong security controls and monitoring mechanisms in place, and keeping lines of communication and collaboration open with providers. Organizations may maximize the advantages of using third-party cloud services while lowering the risks involved and guaranteeing the security and reliability of their cloud environments by resolving these issues [8].

2.5. Theoretical Review

The study employed the deterrence theory to explain the use of cybersecurity to model the factor through cloud computing solutions.

Deterrence Theory

Deterrence theory was developed in criminology and international politics, with early contributions from authors [28]-[30]. The hypothesis proposes that preventing cyber-attacks may be accomplished by putting costs or penalties on attackers, discouraging them from engaging in destructive operations. This theory assumes that individuals or entities are rational agents who consider their actions' possible advantages and hazards before engaging in destructive behavior. Deterrence tactics seek to affect attackers' decision-making processes and dissuade them from engaging in destructive actions by increasing the perceived

risks and repercussions of cyber-attacks [30].

Deterrence Theory may be used to improve cybersecurity with cloud computing solutions by imposing costs on prospective attackers and discouraging them from attacking cloud-based systems. Robust security mechanisms, encryption, and access controls serve as deterrents, raising the perceived risks and repercussions of cyberattacks [31]. Furthermore, cloud computing's scale and flexibility allow organizations to quickly implement and adjust security measures, improving their capacity to respond to emerging threats. Organizations may improve their cybersecurity posture in cloud settings by implementing Deterrence Theory concepts, preventing hostile actors, and encouraging a safer digital ecosystem.

2.6. Empirical Studies Review

[6] attempts to build a viable method for anticipating the use of machine learning in an Industrial Cloud context in terms of trust and privacy. This article focuses on applying machine learning techniques (Support Vector Machine, XG Boost, and Artificial Neural Networks) to improve cloud computing security in the business. The findings showed that the X.G.B. model outperformed across all matrices, with an accuracy of 97.50%, a precision of 97.60%, a recall value of 97.60%, and an F1 score of 97.50%. This study demonstrates ML algorithms' potential to improve companies' cloud computing security.

[32] conducts a comprehensive literature study investigating the implications of digital transformation (DT) and cybersecurity on company resilience. DT entails converting organizational processes to IT solutions, which can result in considerable changes across several parts of an organization. The results demonstrate the necessity of having a thorough understanding of cybersecurity concerns throughout DT deployment to avoid disruptions caused by malicious activities or unauthorized access by attackers seeking to change, destroy, or extort important information from users.

[33] wants to assess significant cybersecurity risks and practices in the cloud across micro, mid, and medium-sized organizations. This study reveals the considerable variances in cloud security procedures across 289 micro, small, and medium-sized firms in Australia, as determined by a survey. It also suggests that future research on cybersecurity challenges and practices in the context of cloud computing should include these distinctions.

3. Methodology

The method adopted for this study encompasses gathering data, conducting necessary cleaning, exploratory data analysis, and model development. The variables considered for the study are all aspects of machine learning in cloud computing security. These variables include Anomaly detection, predictive maintenance, intrusion detection and prevention, and threat intelligence. Based on the data requirements, a survey research design will be adopted, which neces-

sitates going to the field to gather information from participants who can relate to the investigation.

The study population is organizations in prominent industries in selected cities in the United States. Accessibility, data availability, and the feasibility of data collecting are practical considerations that vary between core businesses. It guarantees that the chosen industries will grant the required access and permissions to collect data about the current cloud computing security situation, how effective current security measures are, and how machine learning could improve security. Six hundred cloud professionals across different industries were sent online questionnaires based on their consent to participate in the study. The survey questions of [6] were adopted.

Machine learning algorithms will be utilized, and specifically, the Random Forest Model was used to determine how cybersecurity can be enhanced through cloud computing in the United States due to its several advantages over alternative machine learning methods. [34] [35] Random forest is an ensemble learning method that builds multiple decision trees and merges them to get a more accurate and stable prediction. One of its primary advantages is its ability to handle many input variables without overfitting, making it suitable for complex datasets typical in cybersecurity. Compared to methods like logistic regression or single decision trees, random forests offer higher accuracy, robustness to outliers, and resistance to overfitting. They also provide important insights through feature importance scores, which help in identifying the most critical factors influencing cybersecurity [36]. These attributes make Random Forest a compelling choice for enhancing cloud security. To achieve this, data will be split into train and test sets, features, and targets. The outcome will be evaluated using a confusion matrix, including Accuracy, Precision, and Recall, which are the most used evaluation methods for classification problems.

4. Result and Discussion

The data analysis and machine learning model results are presented in this section.

Table 1 reveals a predominantly male (80.0%) workforce, with females comprising a smaller proportion (20.0%). Regarding age distribution, most fall within the 25 - 34 years bracket (58.7%), followed by those under 24 years (21.6%), indicating a relatively young workforce. Education-wise, a significant portion holds a bachelor's degree (66.0%), while smaller percentages have a master's degree (19.5%) or Doctoral degree (4.4%). Employment status shows a majority in full-time (39.6%) or part-time employment (42.1%), with smaller numbers self-employed, unemployed, or retired. Job roles are diversified, with Cloud Administrators (27.7%), Cloud Architects (25.2%), Cloud Developers (23.0%), and Cloud Engineers (24.1%) being the leading roles. Experience levels vary, with a substantial number having 4 - 6 years of experience (56.9%), followed by 1 - 3 years (20.5%) and over 6 years (17.2%), while fewer have less than 1 year (6.3%).

Table 1. Descriptive analysis of socio-demographic characteristics.

Socio-Demographic Characteristics	Classification	Frequency	Percentage
Gender	Male	710	80.0
	Female	178	20.0
Age	≤24	192	21.6
	25 - 34	521	58.7
	35 - 44	115	13.0
	45 - 54	40	4.5
	>54	20	2.3
Employment status	Unemployed	52	5.9
	Self-Employed	94	10.6
	Full-time	352	39.6
	Part-time	374	42.1
	Retired	16	1.8
Education level	High school	90	10.1
	Bachelor's Degree	586	66.0
	Master's Degree	173	19.5
	Doctor's Degree	39	4.4
Job tenure (in years)	≤1 year	56	6.3
	1 - 3 years	182	20.5
	4 - 6 years	505	56.9
	>6 years	153	17.2
Job Role	Cloud Administrator	246	27.7
	Cloud Architect	224	25.2
	Cloud Developer	204	23.0
	Cloud Engineer	214	24.1

4.1. Feature Selection

The study aims to build a model that predicts how cybersecurity can be enhanced using cloud computing and machine learning. The study employed a random forest model, one of the decision tree models. This was implemented on the dataset based on specific information collected from cloud professionals, providing insights into the ideal steps to boost cybersecurity. Fifteen specific questions were asked. However, when selecting important features, the study considered the correlations between features and potential collinearity problems. The Random Forest Feature Importance was adopted to select the top ten (10) essential features for predicting how cybersecurity can be improved. Each fea-

ture is given a significance score using the Random Forest Feature importance approaches; 10 features are determined to be the most suited based on these scores. This model relies on these features, which are thought to impact its performance significantly or offer helpful information for forecasting the target variable.

The study aims to discover gaps and employ ML models in cloud security, trust, and privacy issues; these features are aimed to cover those bases. The feature scores are displayed graphically below.

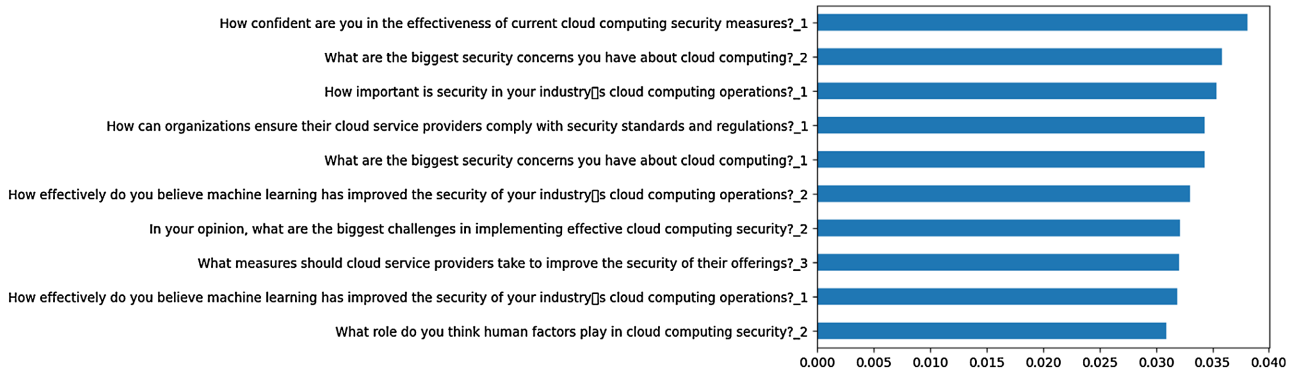

Figure 1. Feature importance score.

4.2. Machine Learning Analysis

Table 2 presents the metrics employed to test the models' performance and their respective scores. The feature importance scores used in the random forest model, as shown in Figure 1, help identify the most critical factors influencing cybersecurity. The study evaluated the models using the F1 score, recall values, accuracy, and precision. Accuracy is defined as the proportion of model variables that are correctly predicted relative to the whole dataset. This statistic alone is insufficient to evaluate the model. Thus, the F1 score, accuracy, and recall metrics must also be considered. Table 2 displays the results of the models that were used.

The Random Forest shows an accuracy of 81.9%. Additionally, it has a precision score of 82.6%, meaning that 81.9% of the model's positive predictions are true positives. The model demonstrates a recall score of 82.1%, which suggests that the actual positive cases correctly identified by the model are 82.1%. On the other hand, the F1 score is 82.1%.

Table 2. Evaluation metrics for the random forest model.

Evaluation Metrics	Scores
Accuracy	0.819
Precision	0.826
Recall	0.819
F1 Score	0.821

Confusion Matrix

The confusion matrix in Figure 2 presents the Random Forest model's performance based on how the targets are classified. Four categories are predicted in the confusion matrix: anomaly detection, intrusion detection and prevention, predictive maintenance, and threat intelligence. The matrix displays the category distribution based on the prediction between the true and predicted labels. 63 examples are correctly categorized as belonging to anomaly detection, whereas 15 instances are wrongly classified. In class 2, 32 occurrences were correctly classified, while 9 cases were mistakenly placed (2 in class 1, 6 in class 3, and 1 in class 4). In class 3, 51 examples are correctly classified, while 9 instances were wrongly placed (7 in class 1 and 2 in class 4). In class 4, 36 cases were correctly placed, while 7 were mistaken for other classes. The confusion matrix reveals that the Random Forest model classification job is based on its understanding of the dataset employed.

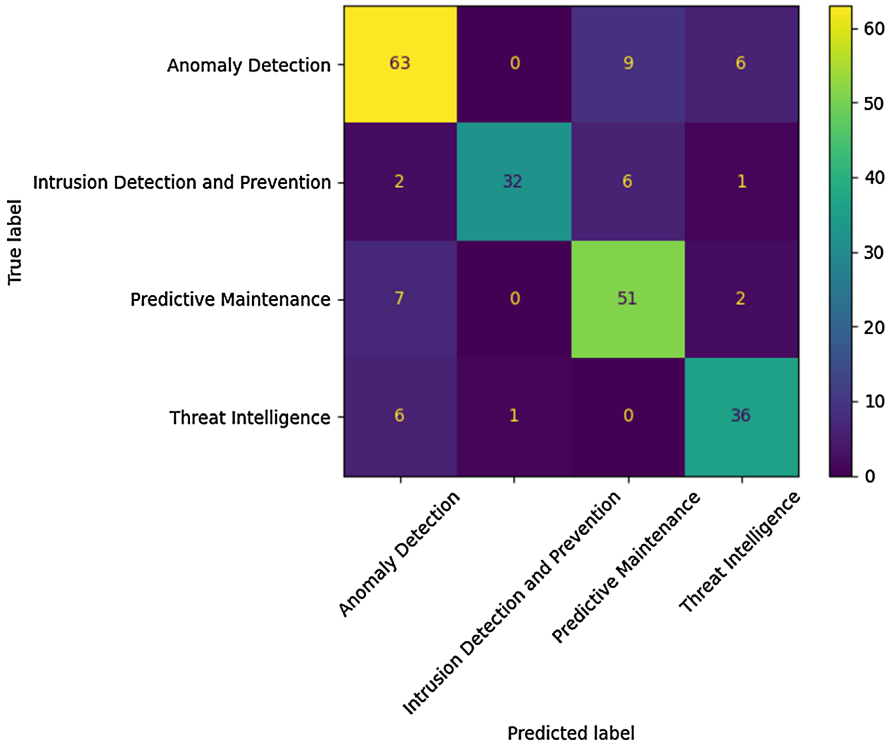

Figure 2. Confusion matrix of Radom forest model.

The random forest performs well based on the evaluation metrics (accuracy, precision, recall, and F1-score). The study employed a machine learning model to predict anomaly detection, intrusion detection and prevention, predictive maintenance, and threat intelligence. Predicting this contributes to enhancing cybersecurity as it relates to specific organizational needs, thereby calling to action the necessary steps to prevent data loss and breaches.

The model performance may call for increasing the dataset; it provides insight into the essential features that contribute to effectively detecting cyberattacks

within the cloud computing niche. Based on this, the random forest model has achieved the study's objective of preventing cybercrime through enhancing cybersecurity.

5. Conclusions and Recommendations

The findings of this study align with existing literature [37]-[39] reinforcing the reliability and practicality of the research conclusions. In the past few years, there has been a noticeable increase in the use of cloud computing for machine learning. The study set out to provide a workable plan for forecasting using ML models in the cloud. A fresh dataset was generated, and the most important features were selected using a feature selection approach known as Random Forest Feature significance. Ten features were identified and included in the actual model trained for prediction. The study employed a Random Forest Classifier as the machine learning model to predict the four categories of improving cybersecurity. The evaluation scores indicated that the model performed well. This can be leveraged by organizations, particularly cloud professionals, to predict possible cyberattacks and the ideal steps to take to prevent them.

Subsequent studies in this area should consider gathering substantial data and adopting other machine learning models to examine how cloud computing can enhance cybersecurity in the United States. Additionally, additional cases and attributes can be added to the dataset. It can help build an accurate and dependable machine learning prediction model for usage in the cloud. Sophisticated optimization methods can boost algorithm training efficiency while maintaining robust privacy, which increases user confidence in cloud computing. Serious collision and reliable but watchful servers can be effectively countered using these tactics. Researchers and developers can tackle issues with cloud computing via federated learning, including confidentiality concerns, high communication costs, statistical volatility, and system diversity.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Butt, U.A., Mehmood, M., Shah, S.B.H., Amin, R., Shaukat, M.W., Raza, S.M., *et al.* (2020) A Review of Machine Learning Algorithms for Cloud Computing Security. *Electronics*, **9**, Article No. 1379. https://doi.org/10.3390/electronics9091379

[2] Ezzat Salem, I. and Hashim Al-Saedi, K. (2023) Enhancing Cloud Security through the Integration of Deep Learning and Data Mining Techniques: A Comprehensive Review. *Periodicals of Engineering and Natural Sciences* (*PEN*), **11**, 176-192. https://doi.org/10.21533/pen.v11i3.3596

[3] O'Donovan, P., Gallagher, C., Leahy, K. and O'Sullivan, D.T.J. (2019) A Comparison of Fog and Cloud Computing Cyber-Physical Interfaces for Industry 4.0 Real-Time Embedded Machine Learning Engineering Applications. *Computers in*

Industry, **110**, 12-35. https://doi.org/10.1016/j.compind.2019.04.016

[4] FBI IC3 Report 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[5] IBM Security (2023) Cost of a Data Breach Report 2023. https://www.ibm.com/security/data-breach

[6] Aljumah, A. and Ahanger, T.A. (2020) Cyber Security Threats, Challenges and Defence Mechanisms in Cloud Computing. *IET Communications*, **14**, 1185-1191. https://doi.org/10.1049/iet-com.2019.0040

[7] Ramos Brandao, P. (2019) Bases, Challenges, and Main Dangers for Deploying Cybersecurity in Industry 4.0. *Advances in Wireless Communications and Networks*, **5**, 33-40. https://doi.org/10.11648/j.awcn.20190501.15

[8] Khan, N. and Al-Yasiri, A. (2016) Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. *Procedia Computer Science*, **94**, 485-490. https://doi.org/10.1016/j.procs.2016.08.075

[9] Sandesh, A. (2022) Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in Our Modern Threat Landscape. *Int. J. Comput. Syst. Eng*, 379-384.

[10] Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., *et al.* (2022) Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information*, **13**, Article No. 146. https://doi.org/10.3390/info13030146

[11] Hassan, W., Chou, T., Tamer, O., Pickard, J., Appiah-Kubi, P. and Pagliari, L. (2020) Cloud Computing Survey on Services, Enhancements and Challenges in the Era of Machine Learning and Data Science. *International Journal of Informatics and Communication Technology* (*IJ-ICT*), **9**, 117-139. https://doi.org/10.11591/ijict.v9i2.pp117-139

[12] Ige, T. and Sikiru, A. (2022) Implementation of Data Mining on Secure Cloud Computing over a Web API Using a Supervised Machine Learning Algorithm. *Proceedings of the Artificial Intelligence Trends in Systems*: *Proceedings of* 11*th Computer Science On-Line Conference*, **2**, 203-210.

[13] Hassan, O.F., Aderibigbe, O.O., Efijemue, O.P. and Onasanya, T.D. (2024) The Impact of Cloud Computing in Promoting Economic Growth through SMEs in the United States. *International Journal of Computer Science and Information Technology*, **16**, 11-23. https://doi.org/10.5121/ijcsit.2024.16202

[14] Vinoth, S., Vemula, H.L., Haralayya, B., Mamgain, P., Hasan, M.F. and Naved, M. (2022) Application of Cloud Computing in Banking and E-Commerce and Related Security Threats. *Materials Today*: *Proceedings*, **51**, 2172-2175. https://doi.org/10.1016/j.matpr.2021.11.121

[15] Abdulshaheed, H.R., Binti, S.A. and Sadiq, I.I. (2018) A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing. *International Journal of Pure and Applied Mathematics*, **119**, 461-486.

[16] Ahmad, W., Rasool, A., Javed, A.R., Baker, T. and Jalil, Z. (2021) Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, **11**, Article No. 16. https://doi.org/10.3390/electronics11010016

[17] Ghobaei-Arani, M., Souri, A., Baker, T. and Hussien, A. (2019) Controcity: An Autonomous Approach for Controlling Elasticity Using Buffer Management in Cloud Computing Environment. *IEEE Access*, **7**, 106912-106924. https://doi.org/10.1109/access.2019.2932462

[18] Su, J. (2019) Why Cloud Computing Cyber Security Risks Are on the Rise: Report. *Forbes*, 25 July 2019. https://www.forbes.com/sites/jeanbaptiste/2019/07/25/why-cloud-computing-cyber-security-risks-are-on-the-rise-report/#13a36bfc5621

[19] Shabbir, M., Shabbir, A., Iwendi, C., Javed, A.R., Rizwan, M., Herencsar, N., *et al.* (2021) Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing. *IEEE Access*, **9**, 8820-8834. https://doi.org/10.1109/access.2021.3049564

[20] Mohiyuddin, A., Javed, A.R., Chakraborty, C., Rizwan, M., Shabbir, M. and Nebhen, J. (2021) Secure Cloud Storage for Medical IoT Data Using Adaptive Neuro-Fuzzy Inference System. *International Journal of Fuzzy Systems*, **24**, 1203-1215. https://doi.org/10.1007/s40815-021-01104-y

[21] Mishra, N., Singh, R.K. and Yadav, S.K. (2020) Analysis and Vulnerability Assessment of Various Models and Frameworks in Cloud Computing. In: Jain, V., Chaudhary, G., Taplamacioglu, M. and Agarwal, M., Eds., *Advances in Data Sciences, Security and Applications*, Lecture Notes in Electrical Engineering, Vol. 612, Springer, 407-417.

[22] Tahirkheli, A.I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., *et al.* (2021) A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. *Electronics*, **10**, Article No. 1811. https://doi.org/10.3390/electronics10151811

[23] Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020) A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. *The Journal of Supercomputing*, **76**, 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

[24] Bhuvaneswary, N., Prabu, S., Tamilselvan, K. and Parthiban, K.G. (2021) Efficient Implementation of Multiply Accumulate Operation Unit Using an Interlaced Partition Multiplier. *Journal of Computational and Theoretical Nanoscience*, **18**, 1321-1326. https://doi.org/10.1166/jctn.2021.9398

[25] Mohammed Sadeeq, M., Abdulkareem, N.M., Zeebaree, S.R.M., Mikaeel Ahmed, D., Saifullah Sami, A. and Zebari, R.R. (2021) IoT and Cloud Computing Issues, Challenges and Opportunities: A Review. *Qubahan Academic Journal*, **1**, 1-7. https://doi.org/10.48161/qaj.v1n2a36

[26] Abbas, Z. and Myeong, S. (2023) Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in Cloud Computing Environment. *Electronics*, **12**, Article No. 2650. https://doi.org/10.3390/electronics12122650

[27] Tahsien, S.M., Karimipour, H. and Spachos, P. (2020) Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey. *Journal of Network and Computer Applications*, **161**, Article 102630. https://doi.org/10.1016/j.jnca.2020.102630

[28] Hobbes, T. (1641) The Third Set of Objections to Descartes Meditations. In: *The Philosophical Writings of Descartes*, Vol. 2, Trans. J. Cottingham, R. Stoothoff and D. Murdoch, Cambridge University Press, 121-137.

[29] Beccaria, C., Newman, G.R. and Marongiu, P. (2009) On Crimes and Punishments. Transaction Publishers.

[30] Moyer, I.L. (2001) Criminological Theory: Traditional and Nontraditional Voices and Themes. Sage.

[31] Wilson, J.Q. and Herrnstein, R.J. (1985) Crime and Human Nature. Simon &

Schuster.

[32] Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A. (2023) Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, **23**, Article No. 6666. https://doi.org/10.3390/s23156666

[33] Nagahawatta, R., Lokuge, S., Warren, M. and Salzman, S. (2021) Cybersecurity Issues and Practices in a Cloud Context: A Comparison amongst Micro, Small and Medium Enterprises. 32*nd Australasian Conference on Information Systems* (*ACIS* 2021), Sydney, 6-10 December 2021, 1-9.

[34] Breiman, L. (2001) Random Forests. *Machine Learning*, **45**, 5-32. https://doi.org/10.1023/a:1010933404324

[35] Liaw, A. and Wiener, M. (2002) Classification and Regression by Random Forest. *R News*, **2**, 18-22. https://www.r-project.org/doc/Rnews/Rnews_2002-3.pdf

[36] Rodriguez-Galiano, V.F., Ghimire, B., Rogan, J., Chica-Olmo, M. and Rigol-Sanchez, J.P. (2012) An Assessment of the Effectiveness of a Random Forest Classifier for Land-Cover Classification. *ISPRS Journal of Photogrammetry and Remote Sensing*, **67**, 93-104. https://doi.org/10.1016/j.isprsjprs.2011.11.002

[37] Nassif, A.B., Talib, M.A., Nasir, Q., Albadani, H. and 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

[38] Gupta, I., Gupta, R., Singh, A.K. and Buyya, R. (2021) MLPAM: A Machine Learning and Probabilistic Analysis Based Model for Preserving Security and Privacy in Cloud Environment. *IEEE Systems Journal*, **15**, 4248-4259. https://doi.org/10.1109/jsyst.2020.3035666

[39] Folorunsho, F.O., Korkor, P.M., Omolola, H.F. and Adeniyi, P.P. (2023) Quantitative Approaches to Forecasting the Economic Impact of Technological Disruptions in Making Informed Decisions for Sustainable Economic Growth in the U.S. *International Journal of Advance Research, Ideas and Innovations in Technology*, **9**. https://www.IJARIIT.com