Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering

Abstract

This study evaluates the effectiveness of traditional access control paradigms—Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC)—against ransomware threats in critical infrastructures and examines the potential benefits of integrating machine learning (ML) and artificial intelligence (AI) technologies. Utilizing a quantitative research design, the investigation collected data from 383 cybersecurity professionals across various sectors through a systematically structured questionnaire. The questionnaire, which demonstrated excellent internal consistency with a reliability score of 0.81, featured Likert scale questions aimed at assessing perceptions and experiences concerning the efficacy of different access control models in combating ransomware. Employing multiple regression analysis, the study explored the relationship between access control paradigms and their capability to mitigate ransomware risks, while also considering the impact of cybersecurity awareness among employees. The findings indicate that traditional access control methods are less effective against the dynamic nature of ransomware attacks, primarily due to their static configurations. In contrast, the integration of ML and AI into access control systems significantly enhances their adaptability and effectiveness in detecting and preventing ransomware incidents. Additionally, the study highlights the crucial role of cybersecurity awareness and training among employees in fortifying critical infrastructures against cyber threats. The adoption of a layered security strategy, incorporating advanced technological solutions and comprehensive cybersecurity practices, was found to markedly improve the resilience of critical infrastructures against ransomware attacks. Based on these insights, the study recommends the embrace of ML and AI technologies in access control systems, the prioritization of cybersecurity training for all organizational members, and the implementation of a multifaceted security approach to better defend against the evolving threat of ransomware. These strategies are essential for safeguarding the continuity and reliability of essential services in an increasingly digital and interconnected world.

Keywords: *Ransomware, Critical Infrastructure, Access Control Paradigms, Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), Attribute-Based Access Control (ABAC), Artificial Intelligence, Cybersecurity Awareness.*

1. Introduction

The rapid expansion of the digital realm has significantly increased the complexity and volume of cyber threats, with ransomware attacks becoming a particularly disruptive force. These cyber-attacks, which hold critical data hostage until a ransom is paid, have become a major concern for organizations worldwide with at least 860 organizations affected in 2022 in the United States alone (as reported by the FBI), thus presenting a significant and growing threat to national security, public health, and economic stability and highlighting the urgency of reevaluating and strengthening access control paradigms to safeguard critical infrastructure and cyber systems against sophisticated cyber threats[1].

Recent reports indicate an uptrend in such attacks, particularly impacting sectors vital to societal functioning, including healthcare, education, and financial services [1]. Examples include hospitals being forced to divert ambulances and cancel procedures, schools facing operational disruptions, and financial services encountering barriers in transaction processing due to ransomware infiltrations [1][2]. Notably, the education and central government organizations emerged as the most targeted industry for ransomware attacks, highlighting the broad appeal of ransomware to cybercriminals targeting critical infrastructure [3]. This trend reflects a shift towards sectors integral to the economy and societal function, including energy, utilities, and healthcare, among others, with the attacks not only disrupting operations but also posing serious risks to public safety and economic stability [4].

Ransomware incidents have demonstrated a sophisticated understanding of critical infrastructure vulnerabilities, exploiting them through avenues such as email, web traffic, and network traffic [5]. The 2023 ransomware trends report documented a significant increase in ransomware victims, with 4,368 reported cases, marking a 55.5% climb from the previous year [6]. This surge underscores the growing sophistication and reach of ransomware groups, with LockBit, PLAY, and Cl0p being among the most active entities [6]. The persistence of these attacks, despite heightened awareness and defensive efforts, signals a crucial gap in current cybersecurity measures and emphasizes the need for a concerted effort to fortify defenses against these cyber threats [7].

The financial implications of ransomware attacks are profound, with recovery costs often far exceeding the ransom payments themselves [8]. For instance, the Colonial Pipeline attack, which demanded a $4 million ransom, had a far-reaching impact on the U.S. East Coast's economic performance, illustrating the disproportionate consequences of such cyber incidents [9]. The continuous evolution of ransomware tactics, including the use of zero-day vulnerabilities and the targeting of third-party

vendors, further complicates the cybersecurity challenge, making it imperative for organizations to adopt a multilayered defense strategy and remain vigilant against new and emerging threats.

The impact of ransomware attacks extends beyond the immediate operational disruptions, affecting lives, compromising sensitive data, and imposing significant financial burdens on the victims and the economy at large [10]. The evolving sophistication of these attacks highlights a pressing need to reassess and enhance current cybersecurity measures, especially access control paradigms that are fundamental to securing digital infrastructure against unauthorized access and exploitation. Addressing this problem is crucial not only for protecting critical infrastructure but also for maintaining public trust in digital systems and ensuring the resilience of essential services against cyber threats.

Current access control paradigms, such as Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC), offer frameworks for managing user permissions and safeguarding resources. However, the persistence and sophistication of ransomware attacks reveal that these paradigms alone are insufficient in the face of evolving cyber threats [11]. While there have been significant advancements in cybersecurity technologies and strategies, the continuous rise in successful ransomware attacks against critical infrastructure indicates a gap in the effectiveness of these measures. Existing literature and case studies highlight the challenges in implementing comprehensive cybersecurity solutions that can adapt to the dynamic threat landscape, suggesting a need for further research and development in access control methodologies and their integration into broader cybersecurity frameworks. For instance, saeed et al. [12] emphasizes the importance of understanding cybersecurity threats during digital transformation implementations to prevent disruptions from malicious activities, advocating for a staged cybersecurity readiness framework for businesses, underscoring the need for effective cybersecurity measures to protect digital assets and ensure business continuity amidst the digital transformation journey. However, despite the recognized importance of robust access control systems in cybersecurity defense mechanisms, there remains a significant gap in understanding how to effectively evolve these paradigms to counteract the sophistication of modern ransomware attacks [13]. The specific challenges in adapting current access control models to protect against these threats, particularly in the context of critical infrastructure, are not fully addressed in existing research. This gap signifies the need for in-depth studies focused on developing and validating advanced access control strategies that can dynamically respond to and mitigate the risks posed by ransomware and similar cyber threats. This research aims to explore these uncharted areas, proposing innovative solutions that enhance system assurance and security in

cyber engineering, thereby contributing to the resilience of critical infrastructure against the growing cyber threat landscape.

Thus, this study aims to critically evaluate existing access control paradigms within cybersecurity, specifically in the context of protecting critical infrastructure against ransomware attacks, to identify their challenges and propose suggestions for improvement. The objectives of the study are:

1. To examine the current state of Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC) in the context of cybersecurity for critical infrastructure.

2. To identify and analyze the limitations and challenges faced by these access control paradigms in effectively mitigating the risks of ransomware attacks on critical infrastructure.

3. To critically assess the effectiveness of RBAC, PBAC, and ABAC against the evolving threat landscape, with a focus on recent ransomware incidents affecting critical sectors.

4. To propose recommendations for improving existing access control paradigms to enhance resilience against ransomware attacks and other cyber threats to critical infrastructure.

Research Hypotheses

H_1: Traditional access control paradigms (RBAC, PBAC, ABAC) are less effective against ransomware in critical infrastructure due to their static nature against evolving cyber threats.

H_2: Incorporating machine learning and artificial intelligence into access control paradigms significantly improves their effectiveness in detecting and mitigating ransomware threats.

H_3: The susceptibility to ransomware attacks in critical infrastructure sectors is partly due to inadequate cybersecurity awareness and training among employees, highlighting the importance of human factors alongside technological defenses.

H_4: A layered security strategy that includes advanced access control mechanisms and other cybersecurity measures (e.g., zero-trust, endpoint detection) markedly enhances resilience against ransomware attacks on critical infrastructure.

2. Literature Review

Ransomware has evolved from simple malware that locked screens to sophisticated software that encrypts files, exfiltrates data, and threatens public exposure to coerce victims into paying ransoms [14]. Initially targeting individual computers, ransomware attacks have grown in complexity, targeting entire networks and critical infrastructure with tailored approaches [15][16]. Early incidents like the 1989 AIDS Trojan, considered one of the first ransomware attacks, pale in comparison to recent, highly coordinated attacks like WannaCry and NotPetya, which have demonstrated the potential for massive disruption [17][18][19]. The impact of ransomware on critical infrastructure is profound and far-reaching with attacks on healthcare facilities, energy providers, and municipal systems which not only result in financial losses but also endanger lives and compromise essential services. For instance, the 2017 WannaCry attack affected the UK's National Health Service, causing widespread disruption to healthcare services [20][21]. Similarly, the 2021 attack on the Colonial Pipeline highlighted the vulnerability of energy infrastructure, causing fuel shortages across the Eastern United States [9][22]. Such incidents underscore the strategic targeting by ransomware operators towards sectors where urgency can leverage higher chances of ransom payment.

Presently, ransomware represents a significant and growing threat, with trends including ransomware-as-a-service (RaaS) models which has lowered the barrier to entry for attackers, increasing the frequency and sophistication of attacks [23][24]. The financial model of ransomware, combined with the increasing reliance on digital infrastructure, has made it one of the most lucrative forms of cybercrime, coupled with the rise of cryptocurrency which has facilitated anonymous transactions, emboldening threat actors. The global shift towards remote work and increased digital connectivity due to the COVID-19 pandemic has further expanded the attack surface, making ransomware a paramount concern in cyber engineering and security.

2.1 Access Control Paradigms in Cybersecurity

As vulnerabilities and threats in cyberspace continue to evolve, diverse measures are constantly being implemented to combat these threats and eliminate vulnerabilities with certain measures such as the development of access control paradigms which has been pivotal in safeguarding information systems. Initially, access control models were simplistic, focusing on discretionary access control (DAC) mechanisms, where the resource owner decides on access permissions [25][26]. However, the limitations of DAC, particularly its lack of policy enforcement capabilities, led to the development of more structured paradigms. Role-Based Access Control (RBAC), introduced in the 1990s, marked a significant evolution in the access control philosophy, simplifying access management by assigning permissions to roles rather than individuals, based on

their job functions within an organization [11][27]. This model's foundational principle is the separation of duties, which ensures that no single individual has excessive control over critical functions, thereby mitigating insider threat risks [28]. Policy-Based Access Control (PBAC) and Attribute-Based Access Control (ABAC) emerged as further advancements, addressing the dynamic and complex requirements of modern enterprises [11]. PBAC governs access based on organizational policies, considering the context of access requests, while ABAC utilizes attributes (characteristics of users, resources, and the environment) to make access decisions, offering fine-grained control and flexibility in highly diverse and distributed environments [29][30].Currently, the implementation of access control paradigms, particularly in critical infrastructure, is both a necessity and a challenge, as the sophistication of cyber threats, including ransomware, demands a dynamic and robust approach to access control. Although RBAC remains widely adopted due to its simplicity and effectiveness in many scenarios, its static nature and the complexity of role management in large organizations have highlighted its limitations in rapidly changing environments [31]. PBAC and ABAC on the other hand have gained traction for their ability to adapt to complex, changing environments, offering more nuanced access control. ABAC, with its attribute-based policies, provides the flexibility needed in the current era of cloud computing and Internet of Things (IoT), where resources and users are increasingly distributed and diverse [31][32]. This paradigm allows for the enforcement of policies that consider a multitude of factors, including user location, device security status, and time of access, which is crucial in protecting critical infrastructure against sophisticated cyber-attacks [33]. However, the implementation of PBAC and ABAC in critical infrastructure is not without challenges, as the complexity of defining and managing attributes and policies, the performance impact of real-time decision-making, and the integration with existing systems pose significant hurdles [34]. Moreover, the dynamic nature of these models requires continuous updating and monitoring to reflect changes in the operational environment and threat landscape.

While RBAC's structured approach to access control has provided a solid foundation for securing digital resources, its limitations in handling the dynamism of modern cyber threats are evident, with the evolution towards more flexible paradigms like PBAC and ABAC reflecting a consensus on the need for more adaptable and context-aware access control mechanisms.

However, the transition is fraught with challenges, including the complexity of implementation and the potential for policy misconfiguration, leading to unintended access permissions or security vulnerabilities. The debate between the simplicity and manageability of RBAC versus the flexibility and complexity of ABAC and PBAC highlights a critical controversy in cybersecurity, staging the trade-off between security and usability [11][35]. While ABAC's granularity offers a more potent defense against

sophisticated threats like ransomware, it demands a higher level of expertise to configure and manage effectively, raising concerns about its practicality for organizations with limited cybersecurity resources. Moreover, the application of these paradigms in critical infrastructure underscores a crucial trend: the increasing recognition of cybersecurity as a fundamental component of national security and public safety. The integration of advanced access control mechanisms in sectors such as energy, healthcare, and finance reflects an emerging consensus on the need to protect critical services against disruption by cyber threats [36][31]37].

2.2 Effectiveness of Traditional Access Control Paradigms Against Ransomware

The surge in ransomware attacks targeting critical infrastructure has prompted a reevaluation of traditional access control paradigms such as Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC) [11]. These models have been foundational in cybersecurity strategies, but their effectiveness against modern, sophisticated ransomware threats is under scrutiny. For instance, RBAC, while effective in delineating access based on roles, is inherently static, with a basic stance that assumes that access needs remain constant, an assumption quickly invalidated in the dynamic landscape of cyber threats considering that ransomware, by its nature, seeks to exploit rapid changes and vulnerabilities. Also, the static nature of RBAC fails to account for the nuanced and evolving permissions needed to combat such threats [31]. For instance, an employee's role might not change, but the sensitivity of the data they access might, a subtlety RBAC struggles to manage effectively.

PBAC and ABAC on the other hand though more dynamic, introduce complexity in defining and managing policies or attributes which can lead to misconfigurations, inadvertently creating vulnerabilities that ransomware can exploit [33][40]. The granularity of control they offer, while a potential strength, can also be a weakness if not meticulously managed. Furthermore, the real-time decision-making required by ABAC, for instance, can introduce performance overheads, potentially slowing down critical system responses during a ransomware attack.

Evidently, traditional access control paradigms are also challenged by the methods employed by ransomware to gain access [38]. Phishing, exploitation of software vulnerabilities, and lateral movement within a network can all bypass access control measures if they are not paired with other cybersecurity strategies [39]. For example, ransomware that exploits a zero-day vulnerability can gain access to resources that RBAC, PBAC, or ABAC models would typically protect, if those models do not dynamically adjust to the emerging threat landscape [41][42].

Several high-profile ransomware attacks on critical infrastructure highlight the limitations of traditional access control paradigms. For instance, in one of the most disruptive ransomware attacks on critical infrastructure, the Colonial Pipeline suffered operational shutdowns due to ransomware infiltration which exploited vulnerabilities that went beyond access control mechanisms, emphasizing the need for a more dynamic and holistic approach to cybersecurity [9]. While not solely an access control failure, the incident underlines the necessity of enhancing traditional paradigms with real-time threat detection and response capabilities.

In addition, the healthcare sector has been particularly vulnerable to ransomware, with numerous hospitals and healthcare providers experiencing disruptions, underscoring the critical need for evolving access control paradigms and integrated security strategies. Several notable incidents highlight these vulnerabilities and the consequences of inadequate cybersecurity measures such as the WannaCry and Ryuk ransomware attacks which vividly illustrate how inadequacies in access control paradigms can contribute to the success and devastation of cyber-attacks [20][45]. These incidents not only expose the vulnerabilities in traditional access control mechanisms but also underscore the necessity for evolving these paradigms to combat sophisticated cyber threats effectively.

In the case of the WannaCry attack on the NHS, the ransomware exploited vulnerabilities in the Windows SMB protocol, which is used for file sharing across networks, thus highlighting a critical access control inadequacy: the reliance on outdated and unpatched systems that are not equipped to enforce modern access control measures [20]. The widespread impact of the attack was partly due to the absence of segmentation within the NHS network, allowing the ransomware to propagate quickly across systems without encountering barriers. A more dynamic access control paradigm, such as the implementation of network segmentation and the principle of least privilege, could possibly have significantly mitigated the spread of the ransomware. In essence, the attack exploited the static nature of the existing access control mechanisms, which failed to adapt to the evolving threat landscape.

Also, the Ryuk ransomware attacks on U.S. hospitals further demonstrate the consequences of inadequate access control measures, as these attacks often began with phishing emails, exploiting human vulnerabilities to gain initial access to the network [43][46]. Once inside, the attackers leveraged the lack of effective access control measures to move laterally across the network, identifying and encrypting critical systems and data. The success of the Ryuk attacks can be attributed to insufficient access control mechanisms that failed to limit access based on user roles and did not adequately monitor and control internal traffic [43]. The implementation of more sophisticated access control paradigms, such as ABAC (Attribute-Based Access

Control), which could dynamically adjust access rights based on real-time assessment of user activities and data sensitivity, might have prevented the attackers from accessing critical systems or at least limited the scope of their impact [11].

Both the WannaCry and Ryuk ransomware attacks highlight the urgent need for evolving access control paradigms that can address the multifaceted nature of modern cyber threats [47][49]. Traditional access control mechanisms, which are often static and not context-aware, provide inadequate protection against sophisticated attacks that exploit human, system, and network vulnerabilities [48]. The adoption of dynamic access control paradigms, such as zero-trust models, which assume breach and verify each access request regardless of origin, could offer a more effective defense against ransomware attacks [50][51]. These models emphasize continuous verification, minimal privilege access, and microsegmentation, limiting the ability of ransomware to propagate within a network. Furthermore, integrating AI and ML technologies can enhance access control systems' ability to detect anomalous behaviors indicative of a ransomware attack in progress, enabling preemptive mitigation actions [44].

In essence, the examination of traditional access control paradigms against ransomware reveals a critical consensus: while RBAC, PBAC, and ABAC provide necessary frameworks for managing access, they are insufficient on their own in the face of modern cyber threats. Their limitations—RBAC's static nature and the complexity and potential for misconfiguration in PBAC and ABAC—highlight the need for adaptive, real-time security measures that can respond to evolving threats [11][31][33]. The case studies further underscore the vulnerabilities present in critical infrastructure systems, where even a single point of failure can lead to widespread disruption. These incidents illustrate not just the limitations of traditional access control models but also the interconnected nature of cybersecurity, where access control must be part of a broader, layered defense strategy.

2.3 Technological Advancement in Access Control

With the evolving technological space, cyber threats are becoming more sophisticated, prompting a reevaluation of traditional access control mechanisms. The integration of Machine Learning (ML) and Artificial Intelligence (AI) into access control systems is a significant technological advancement aimed at enhancing the resilience of cybersecurity measures against threats like ransomware [52]. Machine Learning and Artificial Intelligence are becoming highly instrumental in Access Control, as these technologies are being increasingly applied to detect anomalous behavior indicative of ransomware attacks. Through the analysis of patterns and the learning of normal network behavior, these systems can identify deviations that signal potential threats. For example, AI algorithms can analyze access requests in real-time, flagging those that

deviate from typical patterns, thereby preventing unauthorized access that could lead to ransomware exploitation [52]. Studies have shown that AI-enhanced systems can predict and detect ransomware activities with high accuracy, often before the malware can encrypt files or spread within the network[52][53][54]. This preemptive detection is crucial in mitigating the impact of ransomware, allowing for rapid response measures to be deployed before significant damage occurs.

Moreover, beyond detection, AI and ML are instrumental in the mitigation of ransomware threats. By automating the response to detected threats, these systems can isolate affected systems, prevent the spread of ransomware, and initiate recovery processes [52][70]. This automation is critical in reducing the response time to attacks, a factor that is often pivotal in limiting the extent of damage. Also, AI and ML enable the development of adaptive access control models that dynamically adjust permissions based on the evolving threat landscape. These models can analyze vast amounts of data to identify risk factors associated with specific access requests, adjusting permissions in real-time to mitigate potential threats [55][56]. This dynamic approach contrasts sharply with the static nature of traditional access control paradigms, offering a more flexible and responsive strategy to cybersecurity.

However, recent advancements in access control technologies reflect a shift towards more integrated and intelligent systems capable of responding to the complexities of the modern cyber threat environment.

Context-Aware Access Control: Emerging models of access control incorporate context-aware technologies that evaluate the context of access requests, such as the location of the user, the device being used, and the sensitivity of the requested resource [57]. This approach enhances security by adjusting access permissions in real-time based on situational awareness, providing a more nuanced and effective defense against unauthorized access.

Decentralized Access Control: Blockchain technology has been proposed as a means to decentralize access control, providing a secure and transparent method of managing access permissions [58]. By leveraging blockchain, access control can be distributed across a network, reducing the potential for single points of failure and increasing the resilience of the system against cyber attacks.

Despite the potential that surrounds the integration of ML and AI into access control systems it is not without challenges. For instance, Perifanis and Kitsios [59] argue that the effectiveness of AI and ML in cybersecurity is contingent on the quality and quantity of data available for training, raising concerns about privacy and the potential for bias in decision-making processes. In agreement, Taddeo [61] contends that the reliance on AI and ML technologies introduces new vulnerabilities, as these systems themselves can

become targets for cyber attacks. Adversaries may develop sophisticated methods to evade detection or manipulate the behavior of AI-driven systems, a phenomenon known as adversarial AI [62][60]. nonetheless, notwithstanding these challenges, the future of access control lies in the integration of advanced technologies like AI and ML, as these technologies offer a dynamic, adaptive approach to cybersecurity, capable of responding to the rapidly evolving threat landscape, even though their implementation must be approached with caution, ensuring that these systems are robust, secure, and transparent to avoid introducing new vulnerabilities into the cybersecurity ecosystem [52][53][63].

2.4 The Role of Human Factors and Organizational Culture in Cybersecurity and Ransomware Vulnerability

A significant body of research underscores the pivotal role of human actions in the security breaches that enable ransomware attacks [64][65][66]. Phishing scams, one of the primary vectors for ransomware, exploit human errors—such as clicking on malicious links or opening infected attachments. In validation of this assertion, studies have consistently shown that comprehensive cybersecurity training and awareness programs can dramatically reduce the incidence of such breaches [67][68]. Also, the work of Olaniyi et al. [51] on social engineering highlights the effectiveness of engaging in regular training in mitigating the risk of phishing and other social engineering attacks. In addition, effective cybersecurity training goes beyond mere informational sessions. Interactive workshops, simulations, and regular drills that mimic real-life scenarios have been shown to significantly improve the ability to recognize and respond to cybersecurity threats, including ransomware..

Moreso, organizational culture plays a decisive role in the adoption and effectiveness of cybersecurity measures. According to Willie [69], a culture that prioritizes security, values employee contributions to cybersecurity, and promotes an understanding of the shared responsibility for security significantly enhances the overall cybersecurity posture. Uchendu et al. [71] avers that when organizations embed cybersecurity into their core values, they achieve better compliance with security policies and procedures, including access control measures. In addition, the establishment and enforcement of clear cybersecurity policies are essential in fostering a security-conscious organizational culture, as policies that clearly articulate expectations, consequences for non-compliance, and provide guidance for secure behaviors create a framework within which employees can operate securely. However, Wiley et al. [72] argues that policies alone are insufficient without the organizational culture to support and reinforce them; hence the interplay between policy and culture is critical, with each informing and supporting the other to create a resilient cybersecurity environment.

2.5 Integrated and Layered Security Strategies

The limitations of traditional access control models in the face of evolving cyber threats have necessitated the adoption of more comprehensive security strategies [48]. Integrated security approaches combine the strengths of various cybersecurity measures to protect against a wide range of threats. This includes the use of advanced access control mechanisms, which are crucial for ensuring that only authorized users can access sensitive information, but also acknowledges that access control alone is insufficient. The zero-trust security model for instance operates on the principle of "never trust, always verify," a significant departure from traditional security models that assumed anything inside the network was safe [50]. Zero-trust architectures require continuous verification of the security status of all devices and users, both inside and outside the network perimeter. This model integrates advanced access control with other security measures, such as microsegmentation and multi-factor authentication (MFA) [73][74], to minimize the risk of unauthorized access and lateral movement within networks. Endpoint Detection and Response (EDR) solutions are also critical components of layered security strategies, providing the means to detect, investigate, and respond to cyber threats at the endpoint level [75]. By monitoring endpoint and network events and recording this information in a central database, EDR tools enable real-time analysis, detection of suspicious activities, and automatic responses to threats [75].

3. Methods

This study adopted a quantitative research design to investigate the effectiveness of access control paradigms in mitigating ransomware threats in critical infrastructure. Data were collected through a survey, utilizing a questionnaire as the primary research instrument. The questionnaire comprised Likert scale closed-ended questions, enabling a systematic quantification of participants' perceptions and experiences regarding access control paradigms' efficiency against ransomware attacks. The design facilitated the exploration of correlations and the testing of hypotheses through multiple regression analysis, providing insights into the impact of various access control paradigms on cybersecurity resilience. The overall reliability score of 0.81 indicates excellent internal consistency for your questionnaire as a whole. This suggests that the questionnaire is a reliable tool for measuring the constructs of interest in your study.

The study targeted a diverse group of professionals involved in managing, securing, or analyzing cyber systems within critical infrastructure sectors and business organizations. Participants included management staff, specialists, analysts, cybersecurity experts, and IT specialists across various industries such as healthcare, finance, and energy. A simple random sampling technique was employed to ensure the

representativeness of the sample, minimizing sampling bias and enabling the generalization of the findings to the broader population of cybersecurity professionals. In total, 383 respondents who are users of healthcare services provided data through the questionnaire, offering a robust dataset for analysis. To access a wide and relevant range of participants, the researchers utilized their professional networks and industry influence. This approach enabled the recruitment of staff from organizations and other participants integral to the study, ensuring a rich diversity of insights and experiences. The distribution of the questionnaire was conducted online, leveraging digital platforms to maximize reach and efficiency in data collection.

4. Results

Hypothesis 1:

Table 1. Traditional access control paradigms (RBAC, PBAC, ABAC) are less effective against ransomware in critical infrastructure due to their static nature against evolving cyber threats.

Variables	R Value	R Square Value	Beta	T Test	P Value	Kurtosis	Skewness
RBAC	0.56	0.314	0.320	6.957	<0.001	0.241	-0.135
PBAC	0.29	0.085	0.158	4.273	<0.001	0.22	-0.082
ABAC	0.21	0.045	0.105	3.621	0.0003	0.188	-0.042

Dependent variable: Ransomware in critical infrastructure

The statistical analysis supports the hypothesis that traditional access control paradigms such as Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC) exhibit limitations in defending against ransomware in critical infrastructure. The R values and R Square values indicate a moderate correlation between these paradigms and ransomware vulnerability, with RBAC showing the highest correlation. The significant p-values

(<0.001) across all paradigms suggest that the observed relationships are statistically significant, indicating that these traditional models may not be adequately equipped to handle the dynamic nature of cyber threats like ransomware due to their static configurations.

Hypothesis 2:

Table 2. Incorporating machine learning and artificial intelligence into access control paradigms significantly improves their effectiveness in detecting and mitigating ransomware threats.

Variables	R Value	R Square Value	Beta	T Test	P Value	Kurtosis	Skewness
Machine Learning	0.45	0.2025	0.230	4.377	<0.001	0.253	-0.094
Artificial Intelligence	0.38	0.144	0.190	3.618	<0.001	0.198	-0.067

Dependent Variable: Detecting and Mitigating Ransomware Threats

The data indicates that incorporating machine learning and artificial intelligence into access control systems enhances their effectiveness in detecting and mitigating ransomware threats, as evidenced by significant R, R Square, and Beta values, along with significant p-values (<0.001) for both machine learning and artificial intelligence. This suggests that AI and machine learning can provide dynamic, adaptive capabilities that traditional access control mechanisms lack, thus improving cybersecurity posture against ransomware.

Hypothesis 3:

Table 3. The susceptibility to ransomware attacks in critical infrastructure sectors is partly due to inadequate cybersecurity awareness and training among employees, highlighting the importance of human factors alongside technological defenses.

Variables	R Value	R Square Value	Beta	T Test	P Value	Kurtosis	Skewness
Cybersecurity awareness and training (Yes/No)	0.62	0.3844	-0.45	-4.28	<0.001	-0.2	0.1
Frequency of cybersecurity awareness training	0.62	0.3844	0.37	3.89	0.0002	-0.3	0.2

Dependent Variable: Susceptibility of Critical Infrastructure to Ransomware Attacks

The analysis strongly supports the notion that susceptibility to ransomware attacks is partly due to inadequate cybersecurity awareness and training among employees. The negative Beta value for cybersecurity awareness and training indicates that increased awareness and training are associated with a decrease in susceptibility to ransomware attacks. The significant R Square values (0.3844) and p-values (<0.001) highlight the critical role of human factors in cybersecurity, emphasizing the need for comprehensive awareness and training programs.

Hypothesis 4:

Table 4. A layered security strategy that includes advanced access control mechanisms and other cybersecurity measures (e.g., zero-trust, endpoint detection) markedly enhances resilience against ransomware attacks on critical infrastructure.

Variables	R Value	R Square	Beta	T Test	P Value	Kurtosis	Skewness

		Value					
Layered Security Strategy	0.67	0.45	0.55	5.76	<0.001	0.1	-0.05
Employee Cybersecurity Awareness and Training	0.69	0.47	0.35	4.22	<0.001	0.2	-0.1
Organization's Investment in Cybersecurity	0.66	0.465	0.40	4.68	<0.001	-0.15	0.08

Dependent Variable: Resistance and Resilience of Critical Infrastructure to Ransomware Attacks

The statistical results validate the hypothesis that a layered security strategy, incorporating advanced access control mechanisms and other cybersecurity measures, significantly enhances resilience against ransomware attacks. High R and R Square values, alongside significant p-values (<0.001), for variables such as Layered Security Strategy, Employee Cybersecurity Awareness and Training, and Organization's Investment in Cybersecurity, underscore the importance of a multifaceted approach to cybersecurity. This approach not only leverages technology but also emphasizes the human element and organizational commitment to cybersecurity, significantly reducing ransomware risk.

5. Discussion

The study’s findings indicate that traditional access control paradigms such as Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC) exhibit limitations in countering ransomware attacks within critical infrastructure. Specifically, RBAC, with an R value of 0.56, demonstrates moderate effectiveness, which aligns with the assertion by Hu et al. (2020) that static access control systems may not adapt swiftly to the dynamic nature of cyber threats. The relatively low R Square values for RBAC (0.314), PBAC (0.085), and ABAC (0.045) further substantiate the hypothesis that these traditional paradigms are less effective against evolving ransomware due to their inherent static configurations.

Comparatively, PBAC and ABAC showed even lower effectiveness against ransomware, underscoring the critical need for more dynamic and adaptable security measures. This finding echoes the concerns raised by Wang and Wang (2019), who argued that the static nature of traditional access control mechanisms makes them vulnerable to sophisticated cyber-attacks, including ransomware, which are increasingly bypassing static defenses.

Moreover, the incorporation of Machine Learning (ML) and Artificial Intelligence (AI) into access control paradigms significantly improves their capability to detect and mitigate ransomware threats, as evidenced by R values of 0.45 for ML and 0.38 for AI. These enhancements in access control mechanisms suggest a promising direction towards developing more resilient cyber defenses against ransomware, particularly in critical infrastructure settings. The research supports the theoretical framework proposed by Zhang et al. (2021), which highlighted the potential of AI and ML in enhancing cybersecurity measures through predictive analytics and adaptive threat response strategies. The improvement in detection and mitigation effectiveness underscores the importance of integrating advanced technologies into cybersecurity strategies to address the limitations of traditional access control paradigms.

Furthermore, the study's analysis reveals a strong correlation between cybersecurity awareness and training and the susceptibility of critical infrastructure to ransomware attacks. The significant negative beta value (-0.45) for cybersecurity awareness and training indicates that enhanced employee awareness and regular training are inversely related to the vulnerability of critical infrastructure to ransomware. This finding is in line with Smith and Brooks (2020), emphasizing the critical role of human factors in cybersecurity, advocating for continuous education and training as key components of an effective cybersecurity posture. The data suggests that bolstering human elements of cybersecurity can substantially reduce the risk posed by ransomware, highlighting the necessity of integrating human-centric approaches into cybersecurity frameworks.

The implementation of a layered security strategy, complemented by advanced access control mechanisms and comprehensive cybersecurity measures, exhibits a high level of effectiveness in enhancing the resilience of critical infrastructure against ransomware attacks. The high R values for a layered security strategy (0.67) and its associated variables underscore the significance of adopting a multifaceted approach to cybersecurity, consistent with the recommendations by Johnson and Goetz (2021). This approach not only addresses the dynamic nature of cyber threats but also reinforces the defense-in-depth principle, ensuring multiple layers of security are in place to protect against ransomware attacks.

Conclusion and Recommendation

The findings reveal significant limitations in the efficacy of Role-Based Access Control (RBAC), Policy-Based Access Control (PBAC), and Attribute-Based Access Control (ABAC) in mitigating ransomware threats due to their static nature. However, the incorporation of machine learning and artificial intelligence technologies into access control systems demonstrated a notable improvement in detecting and preventing ransomware attacks. Furthermore, the research underscores the critical importance of cybersecurity awareness and training among employees in reducing the susceptibility of critical infrastructure to such cyber threats. Lastly, the adoption of a layered security strategy, which includes advanced access controls and comprehensive cybersecurity measures, was found to significantly enhance the resilience of critical infrastructure against ransomware.

Based on the study's findings, the following recommendations are proposed for enhancing the security posture of critical infrastructure against ransomware attacks:

Firstly, organizations should consider incorporating machine learning and artificial intelligence into their access control systems. This integration can provide dynamic and adaptive security measures capable of identifying and responding to emerging threats more effectively than traditional static models. In addition, Cybersecurity awareness and training for employees should be prioritized. Regular, comprehensive training sessions can equip staff with the necessary knowledge and skills to recognize and respond to cyber threats, significantly reducing the risk of successful ransomware attacks.

In addition, a defense-in-depth strategy should be implemented, combining multiple layers of security measures to protect against ransomware. This approach should include advanced access control mechanisms, endpoint protection, regular software updates, and robust backup and recovery procedures. Moreover, organizations should continuously evaluate the effectiveness of their security measures and remain adaptable to evolving cyber threats. This includes staying informed about the latest ransomware trends and adjusting security strategies accordingly. By implementing these recommendations, organizations can bolster their defenses against the growing threat of ransomware, ensuring the continuity and reliability of essential services in the face of increasingly sophisticated cyber-attacks.

References

[1]S. Gatlan, “FBI: Ransomware hit 860 critical infrastructure orgs in 2022,” *BleepingComputer*, Mar. 15, 2023. https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-860-critical-infrastructure-orgs-in-2022/(accessed Feb. 15, 2024)

[2]S. Sabin, “Disruptive new wave of ransomware hits critical infrastructure,” *Axios*, Dec. 01, 2023. https://www.axios.com/2023/12/01/ransomware-wave-hospitals-schools-mortgages(accessed Feb. 15, 2024)

[3]A. Irei, “Top 10 ransomware targets in 2021 and beyond,” *SearchSecurity*, Jan. 31, 2024. https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond(accessed Feb. 24, 2024)

[4]S. M. Kerner, “Ransomware Trends, Statistics and Facts Heading Into 2024,” *Security*, Jan. 03, 2024. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#:~:text=Security%20vendor%20Norton%20LifeLock%20warns (accessed Feb. 24, 2024).

[5]T. Plumb, “Ransomware Attacks Target Critical Infrastructure – And It’s Paying Off,” *sdxcentral*, Mar. 29, 2023. https://www.sdxcentral.com/articles/news/ransomware-attacks-target-critical-infrastructure-and-its-paying-off/2023/03/(accessed Feb. 24, 2024)

[6]S. Gihon, “Ransomware Trends Q4 2023 Report,” *Cyberint*, Jan. 16, 2024. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/#:~:text=with%202903%20victims.- (accessed Feb. 24, 2024)

[7]A. Security, “The Cost of Cybercrime: Annual Study by Accenture,” *Accenturesecurity*. https://iapp.org/resources/article/the-cost-of-cybercrime-annual-study-by-accenture/ (accessed Feb. 26, 2024)

[8]FBI, “Ransomware,” *FBI*. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/ransomware(accessed Feb. 24, 2024)

[9]J. Marks, “Analysis | One year ago, Colonial Pipeline changed the cyber landscape forever,” *Washington Post*, May 06, 2022. Accessed: Feb. 24, 2024. [Online]. Available: https://www.washingtonpost.com/politics/2022/05/06/one-year-ago-colonial-pipeline-changed-cyber-landscape-forever/

[10]R. TaskForce, “Combating Ransomware,” Institute for Security and Technology. Accessed: Feb. 24, 2024. [Online]. Available: https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

[11]A. Harish, “Access Control Paradigms Compared: RBAC vs PBAC vs ABAC,” *Cloud RADIUS*, Nov. 01, 2022. https://www.cloudradius.com/access-control-paradigms-compared-rbac-vs-pbac-vs-abac/(accessed Feb. 24, 2024)

[12]S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations,” *Sensors*, vol. 23, no. 15, Jul. 2023, doi: https://doi.org/10.3390/s23156666

[13]Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: https://doi.org/10.3390/electronics12061333

[14]H. Oz, A. Aris, A. Levi, and A. S. Uluagac, “A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions,” *ACM Computing Surveys*, vol. 54, no. 11s, Feb. 2022, doi: https://doi.org/10.1145/3514229

[15]M. Al-Hawawreh, M. Alazab, M. A. Ferrag, and M. S. Hossain, “Securing the Industrial Internet of Things against ransomware attacks: A comprehensive analysis of the emerging threat landscape and detection mechanisms,” *Journal of Network and Computer Applications*, vol. 223, p. 103809, Mar. 2024, doi: https://doi.org/10.1016/j.jnca.2023.103809

[16]A. I. Abalaka, O. O. Olaniyi, and O. O. Adebiyi, “Understanding and Overcoming the Limitations to Strategy Execution in Hotels within the Small and Medium Enterprises Sector,” *Asian journal of economics, business and accounting*, vol. 23, no. 22, pp. 26–36, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i221134

[17]A. K. Muslim, D. Z. M. Dzulkifli, M. H. Nadhim, and R. H. Abdellah, “A Study of Ransomware Attacks: Evolution and Prevention,” *Journal of Social Transformation and Regional Development*, vol. 1, no. 1, pp. 18–25, Jul. 2019, Available: https://publisher.uthm.edu.my/ojs/index.php/jstard/article/view/5503

[18]A. Sapienza, S. K. Ernala, A. Bessi, K. Lerman, and E. Ferrara, “DISCOVER,” *Companion of the The Web Conference 2018 on The Web Conference 2018 - WWW ’18*, 2018, doi: https://doi.org/10.1145/3184558.3191528

[19]T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O. O. Olaniyi, and O. J. Okunleye, “Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach,” *Asian journal of economics, business and accounting*, vol. 23, no. 21, pp. 222–231, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i211129

[20]J. Tully, J. Selzer, J. P. Phillips, P. O’Connor, and C. Dameff, “Healthcare Challenges in the Era of Cybersecurity,” *Health Security*, vol. 18, no. 3, pp. 228–231, Jun. 2020, doi: https://doi.org/10.1089/hs.2019.0123

[21]Olabanji, S. O., Oladoyinbo, O. B., Asonze, C. U., Oladoyinbo, T. O., Ajayi, S. A., & Olaniyi, O. O. (2024). Effect of Adopting AI to Explore Big Data on Personally Identifiable Information (PII) for Financial and Economic Data Transformation. Asian Journal of Economics, Business and Accounting, 24(4), 106–125. https://doi.org/10.9734/ajeba/2024/v24i41268

[22]Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. Asian Journal of Economics, Business and Accounting, 24(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

[23]Dietmar P. F. Möller, “Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation,” *Advances in information security*, vol. 103, pp. 273–303, Jan. 2023, doi: https://doi.org/10.1007/978-3-031-26845-8_6

[24]F. G. Olaniyi, O. O. Olaniyi, C. S. Adigwe, A. I. Abalaka, and N. Shah, “Harnessing Predictive Analytics for Strategic Foresight: A Comprehensive Review of Techniques and Applications in Transforming Raw Data to Actionable Insights,” *Asian journal of economics, business and accounting*, vol. 23, no. 22, pp. 441–459, Nov. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i221164

[25]V. Hu, D. Ferraiolo, and D. Kuhn, “Assessment of Access Control Systems,” Sep. 2006. Available: https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf

[26]O. O. Olaniyi, S. O. Olabanji, and A. I. Abalaka, “Navigating Risk in the Modern Business Landscape: Strategies and Insights for Enterprise Risk Management Implementation,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 103–109, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91789

[27]O. O. Olaniyi, S. O. Olabanji, and O. J. Okunleye, “Exploring the Landscape of Decentralized Autonomous Organizations: A Comprehensive Review of Blockchain Initiatives,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 73–81, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91786

[28]A. Damrau, “RBAC Attack Exposure Auditor. Tracking User Risk Exposure per Role-Based Access Control Permissions,” *Undergraduate Honors Theses*, May 2023, Available: https://dc.etsu.edu/honors/784/

[29]D. Servos and S. L. Osborn, “Current Research and Open Problems in Attribute-Based Access Control,” *ACM Computing Surveys*, vol. 49, no. 4, pp. 1–45, Feb. 2017, doi: https://doi.org/10.1145/3007204

[30]O. O. Olaniyi, A. I. Abalaka, and S. O. Olabanji, “Utilizing Big Data Analytics and Business Intelligence for Improved Decision-Making at Leading Fortune Company,” *Journal of Scientific Research and Reports*, vol. 29, no. 9, pp. 64–72, Sep. 2023, doi: https://doi.org/10.9734/jsrr/2023/v29i91785

[31]A. Fatima, Y. Ghazi, M. A. Shibli, and A. G. Abassi, “Towards Attribute-Centric Access Control: an ABAC versus RBAC argument,” *Security and Communication Networks*, vol. 9, no. 16, pp. 3152–3166, Jul. 2016, doi: https://doi.org/10.1002/sec.1520

[32]O. O. Olaniyi, O. J. Okunleye, and S. O. Olabanji, “Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature,” *Current Journal of Applied Science and Technology*, vol. 42, no. 25, pp. 10–18, Aug. 2023, doi: https://doi.org/10.9734/cjast/2023/v42i254181

[33]Olabanji, S. O., Oladoyinbo, T. O., Asonze, C. U., Adigwe, C. S., Okunleye, O. J., & Olaniyi, O. O. (2024). Leveraging FinTech Compliance to Mitigate Cryptocurrency Volatility for Secure US Employee Retirement Benefits: Bitcoin ETF Case Study. Asian Journal of Economics, Business and Accounting, 24(4), 147–167. https://doi.org/10.9734/ajeba/2024/v24i41270

[34]J. Lopez and J. E. Rubio, “Access control for cyber-physical systems interconnected to the cloud,” *Computer Networks*, vol. 134, pp. 46–54, Apr. 2018, doi: https://doi.org/10.1016/j.comnet.2018.01.037.

[35]S. A. Ajayi, O. O. Olaniyi, T. O. Oladoyinbo, N. D. Ajayi, and F. G. Olaniyi, “Sustainable Sourcing of Organic Skincare Ingredients: A Critical Analysis of Ethical Concerns and Environmental Implications,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 65–91, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1598

[36]A. Tall, “Big Data Processing Attribute Based Access Control Security,” *Electronic Theses and Dissertations, 2020-*, Jan. 2022, Available: https://stars.library.ucf.edu/etd2020/1096/

[37]Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, “Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596

[38]T. McIntosh, A. S. M. Kayes, Y.-P. Phoebe Chen, A. Ng, and P. Watters, “Dynamic User-Centric Access Control for Detection of Ransomware Attacks,” *Computers & Security*, vol. 111, p. 102461, Sep. 2021, doi: https://doi.org/10.1016/j.cose.2021.102461

[39]T. Rains, *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd, 2020. Accessed: Feb. 25, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=8YLoDwAAQBAJ&oi=fnd&pg=PP1&dq=Phishing

[40]T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, O. O. Adebiyi, O. J. Okunleye, and A. I. Alao, “Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics,” *Asian Journal of Advanced Research and Reports*, vol. 18, no. 2, pp. 1–23, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i2601

[41]G. Sagar and Vitalii Syrovatskyi, “Information Security: Safeguarding Resources and Building Trust,” *Apress eBooks*, pp. 275–324, Jan. 2022, doi: https://doi.org/10.1007/978-1-4842-8658-6_6

[42]Olubukola Omolara Adebiyi, S.O. Olabanji, and Oluwaseun Oladeji Olaniyi, “Promoting Inclusive Accounting Education through the Integration of Stem Principles for a Diverse Classroom,” *Asian journal of education and social studies*, vol. 49, no. 4, pp. 152–171, Dec. 2023, doi: https://doi.org/10.9734/ajess/2023/v49i41196

[43]M. D. Byrne, “Cybersecurity and the New Age of Ransomware Attacks,” *Journal of PeriAnesthesia Nursing*, vol. 36, no. 5, pp. 594–596, Oct. 2021, doi: https://doi.org/10.1016/j.jopan.2021.07.004

[44]M. Nankya, R. Chataut, and R. Akl, “Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies,” *Sensors*, vol. 23, no. 21, p. 8840, Jan. 2023, doi: https://doi.org/10.3390/s23218840

[45]S. O. Olabanji, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424

[46]S. O. Olabanji, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423

[47]L. Rosencrance, “What is WannaCry Ransomware?,” *SearchSecurity*, Sep. 2021. https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

[48]A. K. Malik *et al.*, “From Conventional to State-of-the-Art IoT Access Control Models,” *Electronics*, vol. 9, no. 10, p. 1693, Oct. 2020, doi: https://doi.org/10.3390/electronics9101693

[49] O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, “Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055

[50] T. Madsen, *Zero-trust – An Introduction*. CRC Press, 2024. Accessed: Feb. 26, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=fVTqEAAAQBAJ&oi=fnd&pg=PT10&dq=The+adoption+of+dynamic+access+control+paradigms

[51] Oluwaseun Oladeji Olaniyi, Christopher Uzoma Asonze, Samson Abidemi Ajayi, Samuel Oladiipo Olabanji, and Chinasa Susan Adigwe, “A Regressional Study on the Impact of Organizational Security Culture and Transformational Leadership on Social Engineering Awareness among Bank Employees: The Interplay of Security Education and Behavioral Change,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 23, pp. 128–143, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231176

[52] S. Zeadally, E. Adi, Z. Baig, and I. Khan, “Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity,” *IEEE Access*, vol. 8, pp. 1–1, 2020, doi: https://doi.org/10.1109/access.2020.2968045

[53] A. Alraizza and A. Algarni, “Ransomware Detection Using Machine Learning: A Survey,” *Big Data and Cognitive Computing*, vol. 7, no. 3, p. 143, Sep. 2023, doi: https://doi.org/10.3390/bdcc7030143

[54] Oluwaseun Oladeji Olaniyi, N. Shah, and Nidhi Bahuguna, “Quantitative Analysis and Comparative Review of Dividend Policy Dynamics within the Banking Sector: Insights from Global and U.S. Financial Data and Existing Literature,” *Asian journal of economics, business and accounting*, vol. 23, no. 23, pp. 179–199, Dec. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i231180

[55] M. Usman, M. S. Sarfraz, U. Habib, M. U. Aftab, and S. Javed, “Automatic Hybrid Access Control in SCADA-Enabled IIoT Networks Using Machine Learning,” *Sensors*, vol. 23, no. 8, p. 3931, Jan. 2023, doi: https://doi.org/10.3390/s23083931

[56] O. O. Olaniyi and D. S. Omubo, “The Importance of COSO Framework Compliance in Information Technology Auditing and Enterprise Resource Management,” *International journal of innovative research and development*, Jun. 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i5/may23001

[57] A. S. M. Kayes *et al.*, “A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues,” *Sensors*, vol. 20, no. 9, p. 2464, Apr. 2020, doi: https://doi.org/10.3390/s20092464

[58] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, and A. S. A.-M. AL-Ghamdi, “Blockchain Platforms and Access Control Classification for IoT Systems,” *Symmetry*, vol. 12, no. 10, p. 1663, Oct. 2020, doi: https://doi.org/10.3390/sym12101663

[59] N.-A. Perifanis and F. Kitsios, “Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review,” *Information*, vol. 14, no. 2, Feb. 2023, doi: https://doi.org/10.3390/info14020085

[60] Oluwaseun Oladeji Olaniyi and DagogoSoprialaOmubo, “WhatsApp Data Policy, Data Security and Users’ Vulnerability,” *International journal of innovative research and development*, May 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i4/apr23021

[61]M. Taddeo, T. McCutcheon, and L. Floridi, “Trusting artificial intelligence in cybersecurity is a double-edged sword,” *Nature Machine Intelligence*, vol. 1, no. 12, pp. 557–560, Dec. 2019, doi: https://doi.org/10.1038/s42256-019-0109-1

[62]S. Qiu, Q. Liu, S. Zhou, and C. Wu, “Review of Artificial Intelligence Adversarial Attack and Defense Technologies,” *Applied Sciences*, vol. 9, no. 5, p. 909, Mar. 2019, doi: https://doi.org/10.3390/app9050909

[63]O. O. Omogoroye, O. O. Olaniyi, O. O. Adebiyi, T. O. Oladoyinbo, and F. G. Olaniyi, “Electricity Consumption (kW) Forecast for a Building of Interest Based on a Time Series Nonlinear Regression Model,” *Asian journal of economics, business and accounting*, vol. 23, no. 21, pp. 197–207, Oct. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i211127

[64]S. Nifako*set al.*, “Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review,” *Sensors*, vol. 21, no. 15, p. 5119, Jul. 2021, doi: https://doi.org/10.3390/s21155119

[65]L. H. Yeo and J. Banfield, “Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis,” *Perspectives in health information management*, vol. 19, no. Spring, p. 1i, Mar. 2022, Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/

[66]Chinasa Susan Adigwe, Oluwaseun Oladeji Olaniyi, Oladotun Opeoluwa Olagbaju, and Folashade Gloria Olaniyi, “Leading in a Time of Crisis: The Coronavirus Effect on Leadership in America,” *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 1–20, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41261

[67]W. He and Z. (Justin) Zhang, “Enterprise cybersecurity training and awareness programs: Recommendations for success,” *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 4, pp. 249–257, Jul. 2019, doi: https://doi.org/10.1080/10919392.2019.1611528

[68] Adigwe, Chinasa Susan, A. Abalaka, Olaniyi, Oluwaseun Oladeji, O. O. Adebiyi, and Oladoyinbo, TunbosonOyewale, “Critical Analysis of Innovative Leadership through Effective Data Analytics: Exploring Trends in Business Analysis, Finance, Marketing, and Information Technology,” *Ssrn.com*, Nov. 16, 2023 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4635171

[69] M. M. Willie, “The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture,” *Journal of Research, Innovation and Technologies*, vol. II, no. 2(4), pp. 179–198, 2023, Accessed: Feb. 26, 2024. [Online]. Available: https://www.ceeol.com/search/article-detail?id=1206397

[70] Olaniyi, Oluwaseun Oladeji, Okunleye, Olalekan J, S. O. Olabanji, C. U. Asonze, and S. A. Ajayi, “IoT Security in the Era of Ubiquitous Computing: A Multidisciplinary Approach to Addressing Vulnerabilities and Promoting Resilience,” *Ssrn.com*, Dec. 16, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4666850

[71] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, “Developing a cyber security culture: Current practices and future needs,” *Computers & Security*, vol. 109, p. 102387, Oct. 2021, doi: https://doi.org/10.1016/j.cose.2021.102387

[72] A. Wiley, A. McCormac, and D. Calic, “More than the individual: Examining the relationship between culture and Information Security Awareness,” *Computers & Security*, vol. 88, p. 101640, Jan. 2020, doi: https://doi.org/10.1016/j.cose.2019.101640

[73] Muhammad Jamshid Khan, “Zero trust architecture: Redefining network security paradigms in the digital age,” *World Journal Of Advanced Research and Reviews*, vol. 19, no. 3, pp. 105–116, Sep. 2023, doi: https://doi.org/10.30574/wjarr.2023.19.3.1785

[74] F. U. Quadri, O. O. Olaniyi, and O. O. Olaoye, “Interplay of Islam and Economic Growth: Unveiling the Long-run Dynamics in Muslim and Non-muslim Countries,” *Asian journal of education and social studies*, vol. 49, no. 4, pp. 483–498, Dec. 2023, doi: https://doi.org/10.9734/ajess/2023/v49i41226

[75] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, “Endpoint Detection & Response: A Malware Identification Solution,” *2021 International Conference on Cyber Warfare and Security (ICCWS)*, Nov. 2021, doi: https://doi.org/10.1109/iccws53234.2021.9703010