communication between citizens and government institutions, expediting service provision [1].

Moreover, digital transformation can improve government administration and informed decision-making. By providing reliable data and intelligent analysis, the government can make better decisions and foster sustainable development. Techniques like artificial intelligence and data analytics can offer precise policy guidance and enhance government performance, as demonstrated in the Code of Conduct for Good Governance in Public Service (Prime Minister's Decision No. 304 of 2012) [2].

However, challenges must be addressed to successfully develop administrative law in Yemen amidst digital transformation. The country's weak technological infrastructure poses obstacles to the seamless and effective implementation of digital transformation. Investing in technological infrastructure and establishing reliable communication networks are imperative for the success of digital transformation. Additionally, laws and legal frameworks that govern digital technology use, protect personal data, and strengthen cyber security should be developed. New administrative and regulatory laws should also ensure compliance with transparency standards, accountability, and citizens' rights in the digital age.

Furthermore, raising awareness and providing training for government employees on digital transformation and the utilization of digital technology in public administration is crucial. Adequate training and support should be provided to cultivate the necessary digital, technological, and legal skills required to effectively navigate digital transformation.

In conclusion, digital transformation offers significant opportunities for the advancement of administrative law in Yemen, including enhanced transparency, improved government services, and fortified government administration and decision-making. However, addressing challenges related to technological infrastructure, enacting appropriate legal frameworks, and promoting awareness and training are vital to ensure the success of digital transformation in Yemen.

Conclusion

Digital transformation presents a pivotal opportunity for advancing administrative law in Yemen and improving efficiency and transparency in the public sector. However, addressing the aforementioned challenges, including weak technological infrastructure and limited technical skills, is imperative to fully capitalize on these prospects. Furthermore, Yemen should adopt comprehensive strategies and policies to safeguard security and privacy in the digital transformation era. Continuous efforts are required to enhance government capabilities and provide training to employees regarding digital technology and its application in the public sector. In conclusion, digital transformation holds significant potential for enhancing administrative law in Yemen and improving government effectiveness and service delivery. Realizing these potential and surmounting challenges necessitates strong commitment from the government, relevant institutions, and civil society.

References

1. Abdullah Mohammed Al-Gharab.Digital Transformation and its Applications in Public Administration in Yemen (2017).
2. Ali Abdul Karim Al-Sharifi Information Technology and Improving Administrative Laws in Yemen (2016).

CYBERSECURITY AND IMPACT OF DIGITAL TRANSFORMATION

Muqtada Al-Bukari (student)
Al-Saeed University, Taiz, Yemen
Scientific Supervisor – **Raad Al-Selwi**
(Ph.D., Asst. Prof., Al-Saeed University, Taiz, Yemen)

Abstract: The rapid advancement of digital technologies and the widespread adoption of digital transformation initiatives have revolutionized various industries. However, as organizations embrace the benefits of digitalization, they also face the growing challenge of cybersecurity threats. This report explores the critical relationship between cybersecurity and the impact of digital transformation. It examines the vulnerabilities introduced by digitalization, the evolving threat

landscape, and the measures necessary to safeguard sensitive data and systems. By understanding the intersection of cybersecurity and digital transformation, organizations can effectively navigate the complexities of the digital age while mitigating cybersecurity risks.

Key words: Cybersecurity, Digital transformation, Data protection, Threat landscape, Risk management.

Introduction

The ongoing digital transformation has reshaped industries, enabling organizations to streamline operations, enhance efficiency, and provide innovative services. However, this rapid digitalization has also brought about a surge in cybersecurity risks. As organizations embrace digital transformation initiatives, they must prioritize cybersecurity measures to safeguard critical data, protect customer privacy, and ensure the continuity of operations. This report delves into the impact of digital transformation on cybersecurity, highlighting the challenges and opportunities associated with securing the digital landscape.

Results and discussion

Digital transformation introduces new vulnerabilities that can be exploited by cyberthreat actors. The increased connectivity of devices, networks, and systems creates a larger attack surface, making organizations susceptible to cyberattacks. Moreover, the integration of emerging technologies such as cloud computing, Internet of Things (IoT), and artificial intelligence (AI) introduces unique security risks that must be addressed. Organizations must be proactive in identifying and addressing these vulnerabilities to maintain a robust cybersecurity posture [1-2].

The digital transformation era has witnessed a significant evolution in the threat landscape. Cybercriminals are capitalizing on advanced techniques, such as ransomware, phishing, and social engineering, to exploit vulnerabilities and gain unauthorized access to sensitive data. Additionally, state-sponsored actors and organized cybercrime groups are increasingly targeting organizations to steal intellectual property, disrupt operations, or engage in espionage. The dynamic and sophisticated nature of these threats necessitates a comprehensive cybersecurity strategy that includes threat intelligence, proactive monitoring, and incident response capabilities.

Digital transformation involves the collection, processing, and storage of vast amounts of data. Protecting this data and ensuring privacy compliance have become critical concerns. Organizations must implement robust data protection mechanisms, including encryption, access controls, and secure data handling practices. Compliance with privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), is crucial to maintaining customer trust and avoiding regulatory penalties.

Effective cybersecurity in the digital transformation era requires a proactive approach to risk management. Organizations must conduct thorough risk assessments, identify potential vulnerabilities, and implement appropriate security controls. Cybersecurity awareness training for employees is vital to cultivate a culture of security and minimize human error. Additionally, organizations should develop incident response plans, regularly test their resilience through simulations, and establish robust backup and disaster recovery mechanisms to mitigate the impact of cyber incidents.

Conclusion

The impact of digital transformation on cybersecurity cannot be overstated. As organizations embrace the benefits of digitalization, they must simultaneously address the challenges posed by the evolving threat landscape. By prioritizing cybersecurity measures, organizations can protect sensitive data, maintain operational resilience, and build trust with customers. The integration of cybersecurity into digital transformation strategies enables organizations to leverage the advantages of digitalization while mitigating the risks. By adopting a holistic and proactive approach to cybersecurity, organizations can navigate the digital landscape securely and drive innovation with confidence.

References

1. Kshetri, N. (2017). Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. Telecommunications Policy, 41(10), 1027-1038.

2. World Economic Forum. (2020). Cybersecurity Leadership Principles: Lessons Learned During the COVID-19 Pandemic to Prepare for the New Normal. World Economic Forum.

HUMAN MOVEMENT BY USING SIMULATION AND COMPUTER MODELING

Noor Hasan Mohsin Shuaibt
Altinbas University, Turkey
Scientific Supervisor – **Ali Ibrahim Lawah**
(Ph.D., Ministry of Construction, housing, municipalities and public works, Republic of Iraq)

Abstract: Late interest in utilizing demonstrating and reproduction to concentrate on development is driven by the conviction that this approach can give knowledge into how the sensory system and muscles communicate to create composed movement of the body parts. This product gives a stage on which the biomechanics local area can construct a library of re-enactments that can be traded, tried, and worked on through multi-institutional coordinated effort. The outcomes exhibit the possibility of performing computationally effective, prescient, unique streamlining re-enactments of development utilizing full-body, muscle activated models with practical repres sentations of joint capability.

Key words: Musculoskeletal Model, Dynamic Optimization, Collocation, Musculoskeletal, Joint, Muscle Coordination.

Introduction

Researchers intrigued by human and creature development have inspected every one of these means and played out a broad scope of experiments to record neuromuscular excitation patterns, portray muscle-compression mechanics, depict outer muscle math, and evaluate development elements. In stride examination tests, for instance, high velocity camera frameworks are utilized to follow the changing positions and directions of the body sections, strain-check or piezoelectric transducers are utilized to quantify the extents and bearings of the resultant powers applied on the ground. The capacity to perform prescient reenactments is arguably the last fabulous test for bio-researchers and architects intrigued by computational displaying of human development. Model reproductions that anticipate biomechanical capability might support the plan of more successful (designated) work out based treatments for patients with development anomalies coming about because of stroke.

Results and discussion

The information following collocation arrangements precisely recreated the body-segmental relocations, ground response powers and knee contact loads estimated for the two members strolling at their favored velocities. The deliberate pelvic movement was followed RMS blunders < 0.3for revolutions and < 0.3 cm for interpretations while RMS mistakes for all excess summed up organizes were < 2.2 (Table 1 and Fig. 1).

Table 1. RMS errors between model and experiment for two participants walking at their preferred speeds.

Tracking						Non-tracking	
Pelvic motion			Ground reaction force (BW)				
Participant	Rotational ()	Translational (cm)	Fore-aft	Vertical	Mediolateral	Rotational ()*	Knee contact force (BW)
1	0.09	0.27	0.02	0.07	0.02	2.18	0.24
2	0.21	0.20	0.02	0.04	0.02	1.98	0.32