UNITED NATIONS
الاسكوا
ESCWA

Shared Prosperity Dignified Life

BACKGROUND PAPER

Navigating the Future: Building Trust in Digital Government Services Through Emerging Technologies

United Nations publication issued by ESCWA.

Author: Pankaj Pandey.

This background paper was prepared for the Workshop on Building Trust in Digital Government Services, held from 11 to 12 September 2023 in Beirut, Lebanon.

Contents

List of figures

Executive summary

In an era marked by rapid digital transformation, the delivery of public services is undergoing a profound shift, embracing emerging technologies to enhance responsiveness, inclusiveness, trust and effectiveness. This background paper comprehensively examines the critical intersection between technology, trust, and public services. It delves into the core challenges, opportunities, and strategies for building and maintaining trust in an increasingly digitized world. This paper begins with exploring the digital transformation landscape, elucidating the fundamental concepts and drivers behind this transformative process. It highlights the far-reaching implications of digital transformation on public services, from reimagined service delivery models to citizen engagement and data-driven decision-making. Moreover, it identifies and addresses the challenges and opportunities inherent in this profound shift.

Trust is the cornerstone of effective public service delivery. This paper briefly describes the multifaceted notion of trust, examining its importance within government institutions and the evolving dynamics between trust and technology. It underscores trust's pivotal role in fostering citizen engagement and acceptance of digital public services. Furthermore, an extensive overview of emerging technologies, shedding light on their practical applications within public service contexts, is presented. This paper presents a gist of the benefits of the selected emerging technologies, from enhancing operational efficiency to improving service quality, while addressing the inherent risks and ethical considerations associated with their deployment. Therefore, collaboration between government entities and the technology industry is essential to foster trust in digital public services. Also, some compelling examples of exemplary implementations of emerging technologies in public services are provided. These real-world examples offer valuable insights and lessons learned. Finally, this background paper provides a set of recommendations, spanning policy guidance, technological best practices, and capacity building, aimed at guiding governments and organizations toward a future where trust is a cornerstone of their digital service offerings. In conclusion, this paper synthesizes the key takeaways, emphasizing the critical role of trust in the digitalization of public services.

Introduction

"Trust is built in drops and lost in buckets" – Kevin A Plank[1]

In an increasingly interconnected and digitized world, trust has emerged as a foundational concept that underpins the successful delivery of public services. Trust is a multifaceted concept encompassing a sense of reliability, credibility, and integrity in the interactions between government agencies and the citizens they serve. In the context of public services, trust represents the belief that government entities will act in the public's best interests, fulfil their obligations, and protect citizens' rights and information. Trust in the digital age extends beyond traditional notions of interpersonal trust, including trust in technology systems, data handling, and information security. It is not merely about having faith in individuals but also in the systems, processes, and technologies that enable the delivery of public services.

Digital trust is a specialized facet of trust that pertains to citizens' confidence in public services through government organisations as well as associated private sector players' secure and ethical use of digital technologies. It encompasses several critical elements:

- **Data Security**: Citizens trust that their personal and sensitive information will be adequately protected against breaches and unauthorized access.
- **Service Reliability**: Citizens trust that digital services will be available, responsive, and reliable when needed, without disruptions or downtime.
- **Privacy Assurance**: Citizens trust that their privacy rights will be respected, and that data collected for public service purposes will be used responsibly.
- **Transparency**: Transparency in the operations of government agencies and technology systems fosters trust. Citizens expect openness in how public services are delivered and how their data is used.
- **Accountability**: Trust is reinforced when government agencies take responsibility for their actions, including promptly rectifying errors or issues.

Trust and technology are inextricably linked in the digital era. Citizens' trust in government is closely tied to their trust in the technologies used to deliver public services. The relationship between trust and technology can be summarized as follows:

- **Trust Enables Technology Adoption**: Citizens are more likely to adopt and use digital public services when they trust that their data will be handled securely, and their privacy protected.
- **Technology Impacts Trust**: The reliability and security of technology systems directly influence citizens' trust in government entities. Security breaches, data leaks, or service failures erode trust.
- **Ethical Technology Use**: Trust is also influenced by the ethical use of technology. Citizens expect government entities to use technology in ways that align with societal values and ethical principles.
- **Trust as a Competitive Advantage**: Building and maintaining digital trust can be a competitive advantage for government entities. It can enhance citizen engagement, increase service adoption, and improve public perception.

[1] Phone interview with USA Today, February 20, 2014

The lack of trust from the public in emerging digital technologies results in what researchers' term "blind spots" within policymaking procedures[2]. These "blind spots" pertain to policymakers overlooking policy issues due to the public's lack of trust[3]. The public's lack of enthusiasm for emerging technologies can be attributed to inadequate information and limited avenues for public participation. This neglect of public input contributes to the erosion of trust in policies related to emerging technologies[4]. Therefore, as we navigate the complex landscape of emerging technologies in public services, it is imperative to recognize that trust is not static but must be actively nurtured and protected.

One widely cited definition of trust in academia defines trust as *"a psychological state comprising of the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another under conditions of risk and interdependence"*[5]. However, in the context of this paper, we present trust as an analytical model consisting of the ingredients of trustworthiness in digital public services. Since trust comprises multiple dimensions and consists of two interconnected elements[6], namely *trusting beliefs* and *trusting intentions*, we attempt to define trust in digital public services on these two dimensions. In simplified terms, the public will have higher trust in digital public services when the perceived positive belief (hope) on factors like Accountability, Credibility, Reputation, Reliability, Usefulness, Ease of Use, Security, and Privacy increases. However, the public trust in digital public services will decrease when the perceived (wrong) Intentions behind digital public services increase.

Trust = (A + C + Re + R + U + EU + S + P) / I

- **Accountability (A):** Government entities responsible for specific services, compliance, security, data management, privacy, etc., taking responsibility for their actions, both positive and negative.

- **Credibility (C):** Credibility is established at the product or service level, i.e., the credibility of the hardware or software or specific service being offered or frameworks, such as Zero-trust architecture.

- **Reputation (Re):** Reputation is established at the brand level, i.e., the organisation's brand value, providing the digital infrastructure to the government for the delivery of specific digital public services.

- **Reliability (R):** Reliability is rooted in consistency, availability, predictability, and responsiveness without disruptions and downtime.

- **Usefulness (U):** Usefulness is the extent to which the public believes that a particular digital service will offer efficiency and transparency and be effective in eradicating corruption, errors, and delays.

- **Ease of Use (EU):** Ease of use is the extent to which the public believes that using digital public services would be easy for individuals of all age groups, educational levels, languages, digital literacy levels, and the adherence to the system to accessibility requirements.

- **Security (S):** Security is about the cybersecurity of services against any untoward cyber incident and the protection of personal and sensitive information against data breaches and unauthorised access.

[2] Veen and others, 2011.

[3] Ibid.

[4] Kerasidou and others, 2022.

[5] Rousseau and others, 1998.

[6] McKnight and others, 2002.

- **Privacy (P):** Privacy is about the belief of the public that the data collected will be used responsibly and not for irresponsible and unethical use, such as profiling.

- **Intentions (I)**: Intentions in the denominator of the equation refer to the perceived ill-intentions that a private sector vendor, particularly a vendor of foreign origin and the ill-intentions of the government entities, such as snooping, political surveillance, etc., behind a specific digital public service.

I. DIGITAL TRANSFORMATION LANDSCAPE

Digital transformation is a fundamental paradigm shift that has been reshaping the way governments deliver public services. It encompasses a broad spectrum of changes driven by the integration of digital technologies into every facet of government operation, service delivery, and citizen engagement. Understanding the key aspects of digital transformation is crucial as it forms the backdrop against which we explore the implications for public services. The central theme of digital transformation is the transition from analogue and paper-based processes to digital ones. This shift encompasses the digitization of data, processes, and interactions, making it possible to create, store, and transmit information in digital form. This transformation affects every sector of government, from healthcare and education to transportation and public safety.

GovTech[7] embodies a comprehensive government-wide strategy for modernizing the public sector, prioritizing a straightforward, effective, and open government with a strong focus on empowering citizens in the process. This approach stands at the forefront of government digital transformation, setting itself apart from earlier stages by placing a particular emphasis on three key facets of modernizing the public sector:

- Public services that prioritize citizens, ensuring they are universally accessible.

- An all-encompassing government strategy for transforming digital governance.

- Straightforward, effective, and transparent governmental structures.

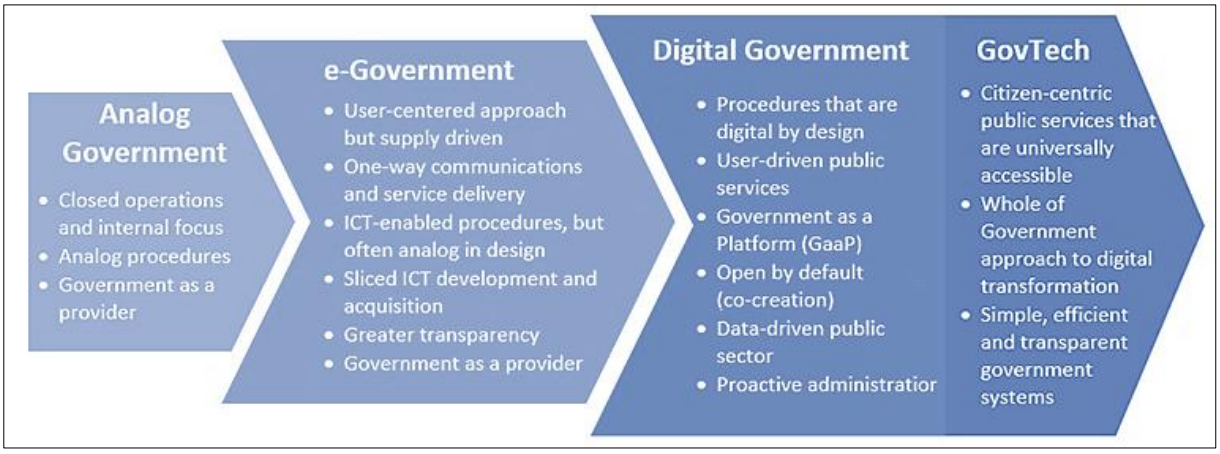
The World Bank, along with client countries and development partners, has employed the phrase "digital government" to delineate the process of modernization and overhaul within the public sector, and some continue to do so. GovTech further advances this concept, as depicted in Figure 1, which illustrates the progression of digital transformation in the public sector. The GovTech agenda also encompasses the proficient utilization of transformative technologies, such as artificial intelligence and machine learning, cloud computing, and the internet of things. Additionally, it encourages the establishment of public data platforms to facilitate the utilization of open public data by individuals and businesses, thus creating value.[8]

The local GovTech ecosystem plays a crucial role in supporting local entrepreneurs and start-ups in developing new products and services for the government. Furthermore, there's a focus on expanding the utilization of public-private partnerships, leveraging private sector expertise, innovations, and investments to tackle public sector challenges. It emphasizes the importance of creating seamless, accessible, and personalized experiences for citizens. This involves leveraging digital channels, such as online portals and mobile apps, to make public services more user-friendly and responsive to individual needs.

[7] World Bank, 2020.

[8] Ibid.

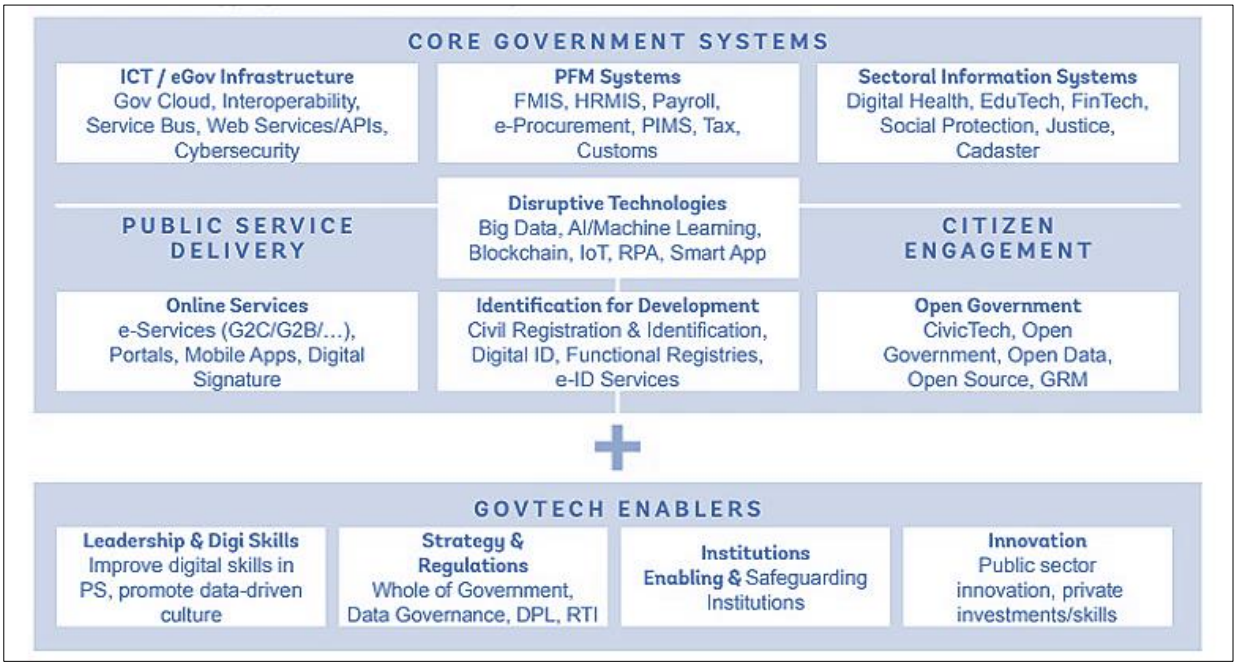
Figure 1. Progression of Digital Transformation



Source: World Bank, 2020.

Automation is a hallmark of digital transformation. It involves the use of technologies like artificial intelligence (AI) and robotic process automation (RPA) to streamline repetitive tasks and workflows. Automation not only reduces operational costs but also enhances the accuracy and speed of service delivery. Figure 2 presents a mapping of digital government investment categories against the GovTech focus areas.

Figure 2. Mapping of digital government investment categories to GovTech focus areas



Source: World Bank, ©2023.

Despite the noted positive effects of digital transformation, the rapid advancement of emerging technologies introduces a risk that only a select few will, enjoy the rewards unless countries invest in fundamental digital infrastructure referred to as Digital Public Infrastructure (DPI)[9]. This infrastructure enables transformative digital solutions, including digital money transfers, online education, and e-health, ensuring accessibility and benefits for every segment of society. DPI is built upon open, interoperable technology and operates within transparent and accountable governance frameworks; it holds the potential to unlock innovation and generate

[9] UNDP and Group of Twenty Presidency, 2023.

substantial value on a large scale while also offering the speed, breadth, and reach required to yield profound societal outcomes that align with progress toward the Sustainable Development Goals (SDGs).

Digital public infrastructure refers to a collection of shared digital systems designed to be secure and interoperable. These systems are constructed based on open standards and specifications and aim to provide broad and fair access to public and private services on a societal level. They are governed by relevant legal frameworks and rules that promote development, inclusivity, innovation, trust, competition, and the protection of human rights and fundamental freedoms[10]. As infrastructure, they depart from the fragmented approach of developing individual digital solutions by promoting interoperable, large-scale initiatives that encourage innovation and competition within this framework[11].

Given the extensive and far-reaching impact of digital transformation on a global scale, the adoption of DPI approaches becomes essential to leverage opportunities for accelerating the Sustainable Development Goals (SDGs) while mitigating the risks associated with digital technologies. The traditional method involves creating specific solutions for distinct issues that work within specific contexts. An alternative approach is to embrace the concept of 'DPI,' which entails employing the right technological architecture and establishing transparent, accountable, and participatory governance systems within local digital ecosystems to drive sustainable innovation and expansion. Through a DPI approach, countries can make progress toward various development goals and respond more effectively in times of crisis.

While each component of DPI can yield individual benefits, the synergy among these infrastructure elements can produce the most significant positive impacts within countries and across the spectrum of SDGs. DPI has the potential to accelerate global economic growth, facilitate the transition to sustainable and environmentally friendly economies, and enhance accessibility and public trust in institutions.

Digital public infrastructure (DPI) can be defined by four key attributes[12]: (1) its interoperability, serving as the foundational structure accommodating a wide array of applications, tools, technologies, and service providers; (2) its adherence to open standards, making it accessible for anyone to expand upon and incorporate services for the benefit of individuals; (3) its operation at a societal level, free from limitations imposed by geographical or demographic constraints; and (4) its strong enabling rules and regulations, ensuring the presence of unified and comprehensive governance frameworks that protect individuals and prevent any misuse. DPI also takes on various forms, and there is a growing consensus on categorizing it into three primary functions[13], with others continually emerging:

- **Digital identity**: This entails the secure verification of individuals and businesses, along with trust-enhancing services like electronic signatures and verifiable credentials.

- **Digital payments**: This involves the easy and instantaneous transfer of funds among individuals, businesses, and government entities.

- **Consent-based data sharing**: This relates to the seamless exchange of personal data between the public and private sectors, all while upholding safeguards for personal data protection in accordance with relevant data governance frameworks.

[10] Ibid.

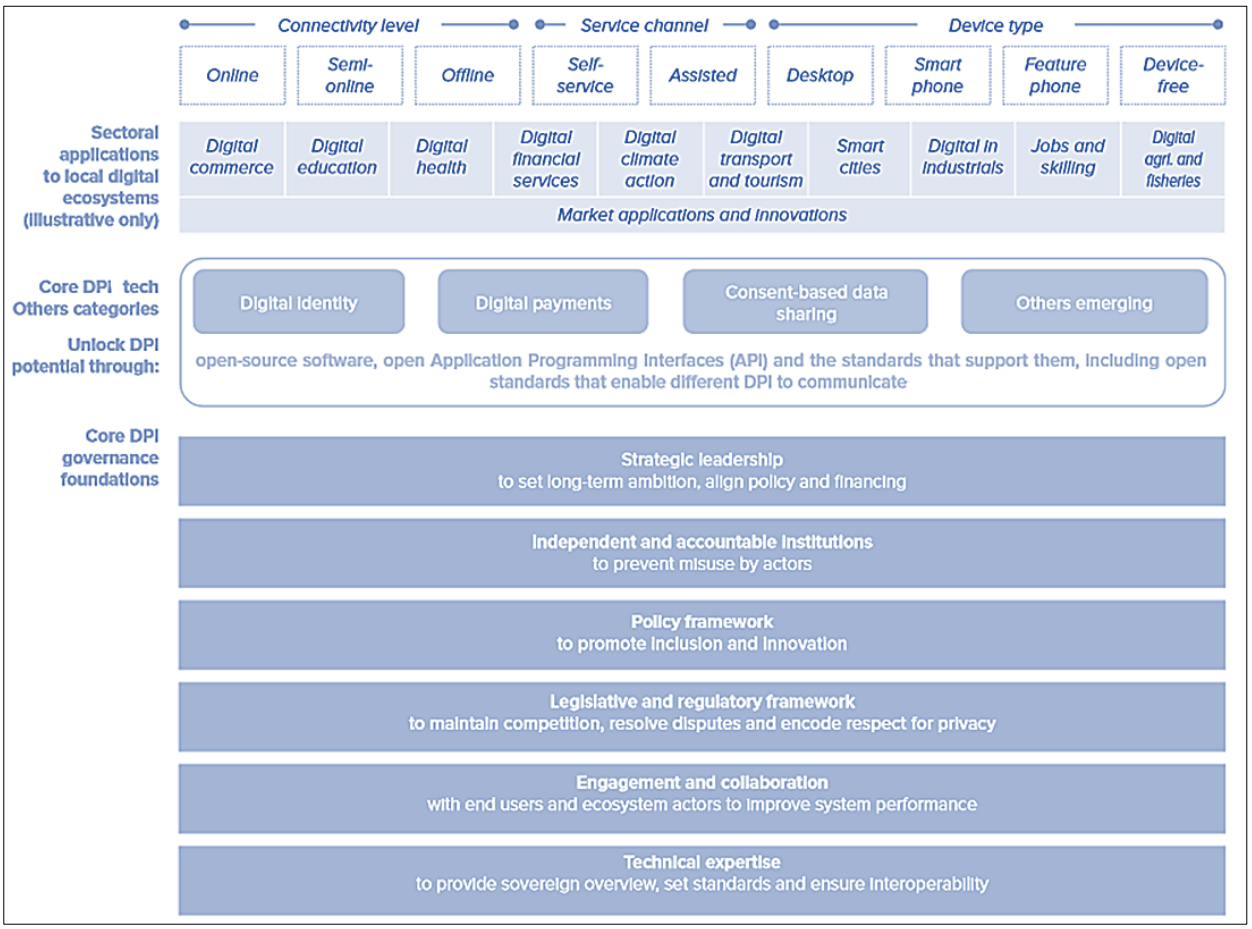
[11] Group of Twenty, 2023.

[12] Ibid. par. 21.

[13] Ibid. par. 17.

- **Other emerging functions**: Additionally, there are other emerging core functionalities of DPI, including but not limited to discovery and fulfilment, geospatial DPI, AI models, and the aggregation of data and content.

Figure 3. A Framework to Understand the DPI Approach



Source: Group of Twenty, 2023

Guidelines: Technology, Governance, and Community Inclusivity[14]

(1) **Inclusivity:** Promote the elimination or reduction of economic, technical, and social barriers to facilitate the inclusion and empowerment of end-users. Ensure last-mile access and take steps to prevent algorithmic bias.

(2) **Interoperability:** Emphasize the importance of interoperability through the utilization and expansion of open standards and specifications, adopting a technology-neutral approach where feasible. This should be done while considering necessary safeguards and being mindful of legal and technical constraints.

(3) **Modularity and Extensibility:** Advocate for an extensible approach, which involves employing a building block or modular architecture that allows for modifications without causing undue disruption.

[14] Ibid.

(4) **Scalability:** Design systems with flexibility to easily accommodate unexpected increases in demand or expansion requirements without necessitating changes to existing infrastructure.

(5) **Security and Privacy:** Incorporate key privacy-enhancing technologies and security features into the core design to ensure individual privacy, data protection, and resilience in accordance with appropriate standards.

(6) **Collaboration:** Encourage the involvement of community stakeholders in various stages of planning, design, construction, and operation. Foster a culture of openness and collaboration to facilitate the development of user-centric solutions and promote widespread adoption while allowing room for innovation.

(7) **Governance for Public Benefit, Trust, and Transparency:** Maximize public benefit, trust, and transparency while adhering to relevant legal frameworks. This entails ensuring the safety, security, trustworthiness, and transparent governance of these systems, promoting competition and inclusion, and upholding principles of data protection and privacy.

(8) **Grievance Redress:** Establish accessible and transparent mechanisms for addressing grievances, including user touchpoints, defined processes, and responsible entities, with a strong focus on taking actions for resolution.

(9) **Sustainability:** Guarantee sustainability by securing adequate financing and technological support, along with enhancements that facilitate uninterrupted operations and the seamless delivery of user-focused services.

(10) **Human Rights:** Adopt an approach that respects human rights throughout the planning, design, construction, and operation phases of these systems.

(11) **Intellectual Property Protection:** Provide effective protection and enforcement of intellectual property rights for the rights-holders of technologies and materials used, in accordance with existing legal frameworks.

(12) **Sustainable Development:** Aim to develop and deploy systems that contribute to the realization of the 2030 Agenda for Sustainable Development and the achievement of Sustainable Development Goals.

II. TRUST IN DIGITAL GOVERNMENT SERVICES

Trust is a foundational element in the relationship between governments and their citizens. In the context of digital public services, trust is not a mere nicety; it is an imperative. Building and maintaining trust are critical for the successful adoption and utilization of digital technologies in the public sector. Trust influences how citizens engage with government services, share information, and perceive the efficacy of their government.

- **Trust and Citizen Engagement**: Citizens are more likely to engage with digital public services when they trust that their interactions will be secure, reliable, and respectful of their privacy. Trust fosters participation in online voting, e-government platforms, and other digital channels for public engagement.

- **Trust and Data Sharing**: Effective public services often require citizens to share personal and sensitive information. Trust is a prerequisite for citizens to willingly provide this data, knowing it will be handled responsibly and used exclusively for its intended purpose.

- **Trust and Public Perception**: The level of trust citizens have in their government directly impacts their perception of government effectiveness. Trust deficits can lead to scepticism, decreased engagement, and reluctance to use digital services.

A. Trust in Government

Trust in government is multifaceted and influenced by various factors. It includes trust in elected officials, government institutions, and public servants. In the context of digital public services, the following aspects are particularly relevant:

- **Transparency**: Transparency in government operations and decision-making processes fosters trust. Citizens expect clear communication about how digital services operate, how data is used, and how decisions are made.

- **Accountability**: Government agencies must take responsibility for their actions. When errors or data breaches occur, a prompt and transparent response can help maintain trust by demonstrating a commitment to resolving issues and preventing future occurrences.

- **Ethical Conduct**: Citizens expect government agencies to use technology ethically. This includes avoiding discriminatory algorithms, protecting individual rights, and ensuring that emerging technologies align with societal values.

B. Trust in Technology

In the digital era, trust extends beyond government institutions to encompass trust in the technologies themselves. Citizens need assurance that the digital infrastructure supporting public services is secure, reliable, and ethical.

- **Security**: Security measures are paramount to building trust in technology. Citizens must trust that their data is protected against unauthorized access, cyberattacks, and breaches.

- **Reliability**: Reliability of digital services is crucial. Downtime, system failures, or glitches erode trust. Ensuring a high level of service availability and performance is essential.

- **Ethical Use**: Ethical considerations surrounding technology use are central to trust. Citizens expect technology to be used in ways that uphold their rights, including privacy, and do not perpetuate bias or discrimination.

C. Trust-Building Strategies

Building and maintaining trust in digital public services requires proactive strategies and measures. These include:

- **Transparency and Communication**: Government entities should communicate clearly about how digital services work, data handling practices, and the steps taken to protect citizens' information. Transparent communication builds confidence.

- **Data Protection**: Rigorous data protection measures, including encryption and access controls, demonstrate a commitment to safeguarding citizen data.

- **Ethical Considerations**: Government entities should prioritize ethical considerations when adopting emerging technologies. Ethical guidelines and impact assessments can help ensure responsible technology use.

- **Accountability**: Accountability mechanisms, such as incident response plans and oversight bodies, are crucial for addressing issues promptly and maintaining trust.

III. EMERGING TECHNOLOGIES IN GOVERNMENT

Emerging technologies are driving a profound transformation in public services, offering governments innovative tools to enhance efficiency, transparency, and citizen engagement. The integration of these diverse emerging technologies holds the potential to revolutionize public services, making them more efficient, accessible, and citizen-centric. To realize these benefits while mitigating risks, governments should prioritize security, ethics, inclusivity, and comprehensive regulatory frameworks in their technology adoption strategies. This section explores a spectrum of pivotal emerging (digital) technologies that are reshaping and likely to drive the future landscape of public service delivery.

(1) **Artificial Intelligence and Machine Learning (AI/ML):** AI and ML empower governments to automate tasks, improve decision-making, and deliver personalized services to citizens.

(2) **Big Data Analysis**: Big Data analytics enable governments to extract actionable insights from vast datasets, optimizing resource allocation and service delivery.

(3) **Blockchain and Distributed Ledger Technology**: Blockchain ensures secure, transparent, and tamper-resistant record-keeping, with applications spanning secure voting systems, supply chain transparency, and government transactions.

(4) **Cloud Computing**: Cloud technology enables scalable and cost-effective IT infrastructure, fostering data accessibility and interagency collaboration.

(5) **Edge Computing**: Edge computing facilitates real-time data processing at the edge of the network, enhancing responsiveness in IoT applications and critical processes.

(6) **Geospatial Technologies**: Geospatial data and technologies facilitate location-based decision-making, benefiting urban planning, disaster management, and environmental monitoring.

(7) **Immersive Technologies**: Immersive technologies like VR and AR enhance citizen engagement and training in fields such as education, public safety, and cultural heritage.

(8) **Internet of Things (IoT):** IoT devices, sensors, and networks enable data collection, automation, and improved service delivery across domains, from smart cities to healthcare.

(9) **Quantum Computing**: Quantum computing holds potential for revolutionizing encryption, solving complex problems, and advancing scientific research.

(10) **6G Technologies**: 6G technologies promise ultrahigh-speed, low-latency connectivity, opening doors for innovative applications in public services, such as real-time remote surgery and augmented reality in public safety.

A. SELECTED USE CASES IN GOVERNMENT SERVICES

Some of the practical applications of emerging technologies across diverse public service domains, as many of these technologies have been implemented by several governments across the globe, are listed below:

(1) **AI/ML in Healthcare**: AI-driven diagnostics and predictive analytics enhance healthcare by enabling early disease detection and personalized treatment.

(2) **Big Data for Social Services**: Big Data analytics inform resource allocation in social services, improving the targeting and efficiency of government social (benefits) programs.

(3) **Blockchain for Transparent Governance**: Blockchain ensures trust and transparency in voting systems, land registries, and government transactions, reducing fraud and corruption.

(4) **Cloud-enabled Government Services**: Cloud computing enables data sharing among government agencies, supporting disaster recovery and remote work capabilities.

(5) **Edge Computing in Public Safety**: Edge computing enhances real-time analysis of video surveillance, aiding law enforcement in crime prevention and response.

(6) **Geospatial Planning**: Geospatial technologies aid urban planning, disaster response coordination, and natural resource management.

(7) **Immersive Learning**: Immersive technologies transform education and training with interactive experiences and simulations, benefiting students and workforce development.

(8) **IoT for Smart Cities**: IoT devices monitor and optimize urban systems, improving traffic management, energy efficiency, and environmental sustainability.

(9) **Quantum Computing for Encryption**: Quantum computing bolsters data security by developing quantum-resistant encryption methods.

(10) **6G for Ultra-Connected Services**: 6G technologies facilitate real-time applications like remote surgery and augmented reality for public safety and healthcare.

B. Benefits and Risks of Emerging Technologies

Governments adopting these emerging technologies must weigh the benefits against the inherent risks to ensure responsible and effective integration; therefore, some core benefits and key risks related to adoption of these emerging technologies for digital public service are listed below:

Benefits

- **Efficiency**: Automation and data-driven decision-making enhance administrative efficiency and resource allocation.
- **Improved Services**: Emerging technologies enable personalized, accessible, and responsive citizen services.
- **Cost Savings**: Cloud computing and automation reduce service delivery costs and infrastructure expenditures.
- **Innovation**: Governments foster innovation ecosystems, stimulating economic growth and global competitiveness.

Risks

- **Security Concerns**: Digitization introduces cybersecurity vulnerabilities and data privacy issues.
- **Privacy Implications**: Data collection raises concerns about citizen privacy and ethical data use.

- **Digital Divide**: Unequal access to technology exacerbates the digital divide, leaving some citizens without vital services.

- **Ethical Considerations**: Responsible AI and technology use must prevent bias, discrimination, and unintended consequences.

- **Regulatory Challenges**: Governments must establish robust regulations and standards to govern the responsible adoption of emerging technologies.

C. Examples of User-Centric Digital Government Services

1. *DigiHelse (Local Government Sector and Norwegian Directorate of eHealth), Norway*

Individuals using home-based services can conveniently and securely connect with their municipal health services through helsenorge.no. They have the ability to send and receive messages, access appointment details, and receive notifications regarding completed home visits. This initiative aims to ensure a consistent service experience for citizens. DigiHelse (DigiHealth) represents a collaborative effort involving the local government sector and the Norwegian Directorate of eHealth Similarly, DigiSos (DigiSocial) is another joint project between the local government sector and the Norwegian Labour and Welfare Administration (NAV). This project focuses on creating digital services for recipients of social assistance through nav.no. The initial service being developed is a digital application for financial assistance, complete with a digital guide.[15].

2. *Virtual Assistants (Public Sector), Australia and Estonia*

Australia and Estonia are presently working on creating customized and smooth services designed for individual users, with a primary emphasis on providing access to data and decisions in a transparent manner. Estonia is in the process of constructing a virtual assistant that complements these services by guiding citizens in their interactions with the public sector. Estonia refers to this as a "human-centric data governance structure." In a similar vein, Australian authorities have introduced their own virtual assistant, offering citizens a more straightforward means of resolving their issues. In both of these instances, government information about citizens is harnessed to tailor intelligent services to individual requirements, regardless of the organizational framework in place.[16]

3. *Public-Private Innovation Partnership (City of Stavanger), Norway*

In an innovation partnership, public and private entities collaborate to create entirely new solutions for current and future societal challenges. This initiative serves as both a legally defined procurement procedure, following the guidelines of the Public Procurement Act., Norway, and a practical framework for fostering dialogue and innovative collaboration with the business sector. The primary objective is to develop innovative products and solutions that are currently unavailable in the market. The foundation of an innovation partnership is rooted in identifying public needs, securing top management support, and involving both the business and public sectors in comprehending these needs and devising solutions.

The City of Stavanger has become the first in Norway to experiment with this novel form of competitive innovation partnership[17]. The journey began when the City of Stavanger sought fresh and inventive solutions to enhance the engagement and coping abilities of individuals on short-term stays in nursing homes. Even a mere one-week stay in bed leads to a 10 percent decrease in stamina and a 20 percent decline in muscle strength. Currently, short-term stays incur an annual cost of NOK 200 million for the city. The potential for

[15] Government of Norway. Ministry of Local Government and Modernisation, 2019.

[16] Ibid.

[17] Ibid.

savings through reduced stays and fewer readmissions is substantial. Through the innovation partnership, the business sector has collaborated closely with the city to develop a smart wheeled walker and/or activation robot. Once the development phase is complete, the contracting authority can choose to acquire the solution without the need for competitive tendering, and the project is presently in the negotiation phase for procurement. Notably, this project has spawned three subsidiary enterprises – the municipalities of Kristiansand and Bærum, as well as NAV Assistive Technology – all of which may also opt to acquire these solutions if they desire.

4. *Surveillance of E-commerce for Dangerous Products (Sikkerhedsstyrelsen – a Government Agency), Denmark*

Sikkerhedsstyrelsen's surveillance of online commerce for the detection of hazardous items involves the utilization of Machine Learning and Image Recognition technologies to spot potentially unsafe and unlawful products being distributed on the internet The initial project has provided clear documentation indicating that the AI solution outperforms the traditional manual process in terms of effectiveness and accuracy. In a bid to enhance and expand cooperation among public bodies, this AI solution will be expanded to encompass additional domains related to monitoring online markets.[18].

5. *Motorway monitoring with AI Image Recognition (ASFINAG - Motorway Infrastructure), Austria*

ASFINAG employs artificial intelligence (AI) and Image Recognition for tasks related to Austria's motorway infrastructure. This includes AI applications for recognizing toll stickers and license plates. The technology also holds promise for real-time identification of hazardous conditions on the roads, particularly within tunnels, as well as for optimizing traffic flow and conducting infrastructure assessments. In contrast to conventional software, the results and effectiveness of AI in specific use cases are unpredictable and often cannot be predetermined in advance.[19]

6. *Medical Decision Support Through Automatic Image Recognition (IRCCS Policlinico San Donato University Hospital), Italy*

The organization is in the process of testing AI in the fields of diagnostic imaging and electrocardiography. The automated interpretation of images allows radiologists to focus on analysing intricate pathologies. For medical professionals, these AI tools are increasingly integral to decision support, enabling the customization of treatment plans. While still in the experimental phase, these AI diagnostic solutions, among others, are already proving to be highly beneficial for the medical staff.[20]

7. *Automatic Intelligent Extraction of Unstructured Data (Colegio de Registradores - Public Law Corporation), Spain*

The Colegio de Registradores is employing automated intelligent extraction of data using Natural Language Processing to convert unorganized data from PDF documents into an organized format This leads to streamlined data processing. The adoption of this solution brings immediate advantages, including cost reduction and time savings in document processing. Furthermore, it facilitates the integration of organized data into databases and management applications, potentially yielding additional advantages and service improvements.[21].

[18] Bertrand and others, 2020.

[19] Ibid.

[20] Ibid.

[21] Ibid.

8. *Experimenting with Deep Learning & Computer Vision (Vlaamse Overheid - Regional Government), Belgium*

The Flemish Government has established multiple programs and test endeavours in the realm of Computer Vision. These initiatives utilize Image Recognition and Image Processing to enhance the pace and volume of insights that public entities can generate from existing geospatial data. A strong partnership between various departments within the Flemish government, each possessing geospatial image resources, forms the basis for further AI undertakings.[22]

9. *Big Data Supporting Medical Decisions (CHUSJ - University Hospital), Portugal*

The project leverages big data for the enhancement of patient diagnoses and treatment. It achieves this by conducting extensive analysis of unorganized data that would otherwise be challenging to handle. An AI-driven data mining platform is employed to automatically interpret recorded patient data, employing keywords to label patient conditions, allergies, surgeries, and medication. This process creates a readily accessible patient profile for the physician.[23]

10. *Inspecting bridges and viaducts using drones and AI (Rijkswaterstaat - Agency for Infrastructure and Water Management), The Netherlands*

The examination of bridges and viaducts involves the utilization of drones and Deep Learning techniques to identify structural harm. Drone inspections are safer compared to manual assessments. With the information obtained, Rijkswaterstaat can determine whether specific damage requires immediate attention or can be included in regular maintenance schedules. Through Deep Learning, the substantial volume of visual data generated can also be examined to continuously enhance performance.[24]

11. *Public Service innovation through AI (Department of Public Expenditure and Reform - Federal Government), Ireland*

The Irish Revenue Commissioners explored the use of AI to deliver a more streamlined and proficient public service to taxpayers. They initiated a pilot project that introduced a Virtual Digital Agent powered by Natural Language Processing. The pilot project promptly demonstrated its worth, which led to its complete implementation. During this initiative, as many as half of the calls were managed entirely by the voice Bot, from the beginning to the end. Only a mere 10 per cent of calls required transfer to a human agent due to difficulties in comprehending the spoken information.[25]

12. *Unique Identification Authority of India (Aadhaar - Government of India), India*

Aadhaar, India's Digital Public Infrastructure (DPI), plays a crucial role in establishing trust by democratizing the foundational ability to verify an individual's identity accurately[26]. Aadhaar promotes interoperability, is constructed on open standards, and provides a controlled environment for innovation, allowing both public and private service providers, including mobile network providers and financial institutions, to seamlessly integrate their systems. It operates under robust governance frameworks, enabling the country to make necessary updates easily in response to evolving demands and requirements. During the

[22] Bertrand and others, 2020.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] n 17

pandemic, Aadhaar played a significant role in empowering underprivileged individuals by facilitating direct benefit transfers and democratizing access to essential public services such as education, public food distribution, and public sector wages.

Notably, using digital ID systems for public sector wage payments has proven effective in plugging payment leaks, resulting in increased public sector wages and up to a 13.4% improvement in household incomes. Several other digital ID DPI approaches, like Ethiopia's National ID and the Philippines' ePhilID, built on the MOSIP (Modular Open-Source Identity Platform) – a Digital Public Good (DPG), serve similar functions to Aadhaar.

13. *MIZAN (Access to Justice), Palestine*

Palestine's MIZAN[27], a digital case management system, enhances access to justice by providing comprehensive case management services. This includes overseeing judges' schedules and document flows, enabling payments, and allowing complainants to monitor the progress of their cases. Multiple government departments can access this service. MIZAN fosters better coordination among government agencies and legal aid organizations, fostering transparency and trust within the judicial system. Users can monitor their disputes and make digital payments online. This improved transparency has also led to a reduction in corruption among judicial officials.

In a similar vein, the Brazilian Government has introduced Consumidor, an online alternative dispute resolution system. This platform provides a secure and transparent environment where consumers can register and oversee their grievances with service providers. Consumidor not only bolsters consumer trust in the market but also fosters transparency and enhances the effectiveness of redressal systems. Since its inception, Consumidor has recorded close to 6 million complaints, with an impressive 77 per cent of them successfully resolved within seven days. Additionally, by making complaint data publicly available, Consumidor contributes to evidence-based policymaking concerning redressal mechanisms.

14. *PRISM and Global Forest Watch, Indonesia, Sri Lanka, Mongolia, Cambodia, and others*

PRISM, which stands for the "Platform for Real-time Information and Systems Monitoring," is a Digital Public Good (DPG) that furnishes real-time data for governments and organizations. This data empowers them to monitor and respond effectively to climate- and weather-related threats such as floods, landslides, and droughts. PRISM operates on a societal scale and serves multiple countries, including Indonesia, Sri Lanka, Mongolia, and Cambodia. Notably, it has integrated fifteen climate monitoring products. Moreover, PRISM boasts interoperability with the KOBO toolbox.[28]

Similarly, Global Forest Watch (GFW) is a digital system that leverages geospatial data to generate deforestation alerts in near-real-time. GFW facilitates access to open data through open APIs, allowing for the development of customized applications. It has gained adoption in nearly 25 countries. GFW plays a crucial role in disseminating verified information that encourages evidence-based community actions aimed at curbing unsustainable deforestation. It involves training members of local communities to identify and combat unauthorized deforestation. The generated alerts are shared with local communities both digitally and through analogue systems, ensuring that critical information reaches areas with limited digital penetration and network access.[29]

[27] Ibid.

[28] WFP, 2022.

[29] Global Forest Watch, n.d.

15. *TradeTrust and SGFinDex, Singapore*

Singapore's TradeTrust is founded on the blockchain-driven DPG OpenAttestation platform, designed for exchanging trade documents between governments and businesses and document verification. This innovative system has undergone successful pilot implementations in five different countries. Importantly, TradeTrust is designed to integrate with the backend of existing open-source systems seamlessly. By doing so, it streamlines business operations and enhances the effectiveness and flexibility of supply chains. Notably, it has managed to reduce the time required for trade processes from over ten days to less than a single day.[30]

Similarly, Singapore's SGFinDex serves as the bedrock infrastructure for digital finance, prioritizing the security and protection of users. It empowers individuals to access and comprehend how their financial data is utilized by both government agencies and private service providers. With a significant 30,000 monthly active users, this platform facilitates data sharing through open data standards and APIs. Moreover, its OAuth 2.0 authorization framework allows third-party applications to secure user consent and access data on the user's behalf. SGFinDex seamlessly integrates with the National Digital Identity SingPass for authorization purposes.

16. *Quantum Computing Algorithms for Next-Generation Mobile Networks (Telecom Italia), Italy and China*

The COVID-19 pandemic has underscored the critical need for ensuring fair access to broadband internet and enhancing mobile connectivity, and quantum computers can play a role in addressing this issue. The Department for Digital, Culture, Media, and Sport (DCMS) has long been dedicated to the expansion of broadband and the rollout of 5G networks[31]. However, there is room for further progress by integrating quantum-hybrid applications.

Telecom Italia stands out as the first telecommunications operator in Europe to incorporate quantum computing algorithms into the planning of their next-generation mobile networks. In collaboration with D-Wave, the company optimized the implementation of telecom infrastructure, achieving the task "ten times faster than conventional optimization methods." Beyond the increased efficiency, quantum computers enable the adaptability of such solutions, allowing for real-time network configuration and enhancements in service quality.[32]

The China Mobile Research Institution (CMRI) and Origin Quantum Computing Technology Co. have achieved the initial instance of algorithm verification utilizing a genuine universal quantum computer within China. China Mobile is presently engaged in 5G operations and the research and development of 6G. In contrast to 5G, 6G will encounter significant computational hurdles encompassing extensive service optimization, network optimization, signal processing, and the training of large machine models. Consequently, the existing computational methods and algorithms will be under immense strain.[33]

IV. ZERO-TRUST ARCHITECTURE IN PUBLIC SERVICES

Zero-Trust Architecture (ZTA) represents a modern and effective approach to cybersecurity in public services. By implementing ZTA principles, government entities can enhance security, protect sensitive data, and adapt to the changing threat landscape. As digital public services continue to evolve, a commitment to trust and security remains paramount. Therefore, the future of Zero-Trust Architecture in public services may include advancements in automation, AI-driven threat detection, and improved user experience through secure access methods. Zero-Trust Architecture (ZTA) is a security model that challenges the traditional perimeter-

[30] n 17.

[31] Lopez, 2022.

[32] TIM Group, 2020.

[33] Global Times, 2023.

based approach to cybersecurity. In a zero-trust model, trust is never assumed, and verification is required from anyone trying to access network resources, regardless of location. Zero-Trust Architecture offers several applications within public services:

- **Secure Remote Access**: With the rise of remote work, ZTA ensures that remote users must authenticate and adhere to security policies before accessing government systems and data.
- **Protecting Sensitive Data**: ZTA helps safeguard sensitive government data by enforcing strict access controls and encryption measures.
- **Critical Infrastructure Security**: Government entities responsible for critical infrastructure, such as power grids and transportation systems, rely on ZTA to defend against cyber threats.
- **Public-facing Services**: Zero-trust principles apply to public-facing government websites and services, ensuring secure interactions with citizens and businesses.

However, implementing Zero-Trust Architecture in public services is not without challenges:

- **Complexity**: ZTA implementation can be complex, requiring a thorough understanding of network infrastructure and robust identity and access management solutions.
- **User Experience**: Striking a balance between security and user experience is crucial. Stringent security measures should not hinder productivity or citizen interactions.
- **Legacy Systems**: Many government agencies have legacy systems that may not easily adapt to ZTA principles. Transition strategies are needed.

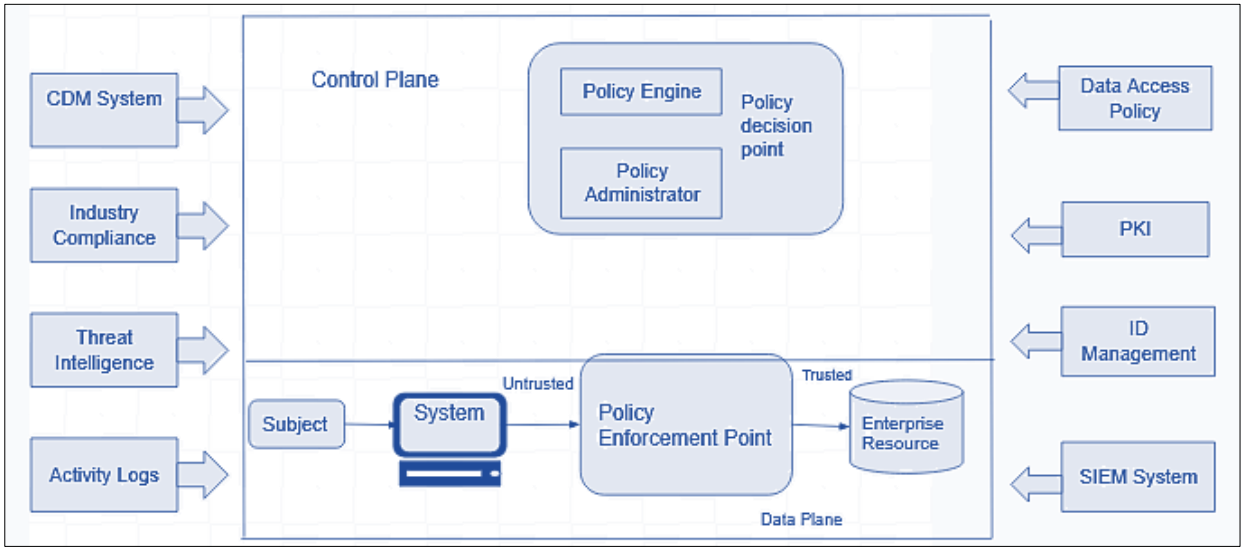
Despite the aforementioned challenges in the implementation of ZTA in public services, the adoption of the same offers the following unique benefits which could be crucial in building trust among the public:

- **Enhanced Security**: ZTA minimizes the attack surface and reduces the risk of data breaches and cyberattacks.
- **Data Protection**: Sensitive government data is better protected, ensuring compliance with data protection regulations.
- **Adaptability**: ZTA is flexible and adaptable, making it suitable for evolving digital public service environments.

A ZTA deployment within an enterprise comprises numerous logical elements. These elements can function either as an on-site service or through a cloud-based service. Figure 4 illustrates a conceptual framework model, demonstrating the fundamental connections between these elements and how they interact[34]. It's important to note that this model is an ideal representation showcasing logical components and their interactions. In the ZTA architecture, the logical components utilize a distinct control plane for communication, while application data is transmitted via a separate data plane.

[34] Rose and others, 2020.

Figure 4. Core Zero trust Logical Components



Source: Rose and others, 2020.

The component descriptions are as follows[35]:

- **Policy Engine (PE):** The PE is responsible for making the final decision regarding whether a subject should be granted access to a particular resource. It uses enterprise policies and external inputs (such as data from CDM systems and threat intelligence services) as inputs for a trust algorithm. Based on this, it determines whether access should be granted, denied, or revoked. The PE works closely with the policy administrator component. It not only makes the access decision but also logs it, and the policy administrator carries out the decision.

- **Policy Administrator (PA):** The PA plays a key role in establishing or terminating the communication path between a subject and a resource. It issues commands to relevant Policy Enforcement Points (PEPs) to enable or disable these connections. Additionally, the PA generates session-specific authentication and authorization tokens or credentials that clients use to access enterprise resources. Its actions are closely linked to the PE's decisions, as it relies on these decisions to allow or deny a session. If a session is authorized and the request is authenticated, the PA configures the PEP to permit the session to commence. Conversely, if the session is denied or a prior approval is reversed, the PA instructs the PEP to terminate the connection. In some implementations, the PE and PA may be considered a single service, but here, they are treated as two distinct logical components. The PA communicates with the PEP when setting up the communication path, and this communication occurs through the control plane.

- **Policy Enforcement Point (PEP):** The PEP is responsible for enabling, monitoring, and, when necessary, terminating connections between a subject and an enterprise resource. It interacts with the PA to relay access requests and receive updates regarding policies. In ZTA, this is considered a single logical component, but it can be divided into two different components: the client side (e.g., an agent on a laptop) and the resource side (e.g., a gateway component in front of the resource that controls access). Alternatively, it can be implemented as a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP lies the trust zone where the enterprise resource is hosted.

[35] Rose and others, 2020.

In addition to the essential components within an enterprise implementing ZTA, various data sources contribute input and policy rules for the policy engine to use when making access decisions. These sources encompass both local data sources and external ones, which are not under enterprise control or creation. These can encompass the following elements[36]:

- **Continuous Diagnostics and Mitigation (CDM) System**: The CDM system compiles data on the current state of enterprise assets and implements updates to configurations and software components. It supplies the policy engine with information regarding assets making access requests, including details like whether they run the correct, up-to-date operating system, the integrity of approved software components, the presence of unapproved components, and any known vulnerabilities. CDM systems also play a role in identifying and, in some cases, enforcing policies on non-enterprise devices active within the enterprise infrastructure.

- **Industry Compliance System**: This system ensures that the enterprise remains in compliance with applicable regulatory frameworks (e.g., FISMA, healthcare, or financial industry information security requirements). It encompasses all the policy rules developed by the enterprise to ensure compliance.

- **Threat Intelligence Feeds**: These sources provide information from both internal and external outlets to assist the policy engine in making access decisions. They can consist of multiple services that gather data from various internal and external sources, offering insights into newly discovered attacks or vulnerabilities. This includes newly identified software flaws, newly detected malware, and reported attacks on other assets that the policy engine may want to block access from enterprise assets.

- **Network and System Activity Logs**: This enterprise system aggregates logs from assets, network traffic, resource access activities, and other events to offer real-time or near-real-time feedback on the security status of enterprise information systems.

- **Data Access Policies**: These are rules, attributes, and policies governing access to enterprise resources. These rules can be encoded through a management interface or dynamically generated by the policy engine. They serve as the foundational access privileges for accounts and applications/services in the enterprise, and they should align with the defined mission roles and organizational needs.

- **Enterprise Public Key Infrastructure (PKI):** This system is responsible for generating and recording certificates issued by the enterprise to resources, subjects, services, and applications. It includes the global certificate authority ecosystem and the Federal PKI, which may or may not be integrated with the enterprise's PKI. It might also utilize PKI structures not based on X.509 certificates.

- **Identity Management System (ID Management System):** This system manages the creation, storage, and administration of enterprise user accounts and identity records, often utilizing components like Lightweight Directory Access Protocol (LDAP) servers. It stores subject information such as names, email addresses, certificates, as well as enterprise-specific attributes like roles, access permissions, and assigned assets. This system might be part of a larger federated community and could involve non-enterprise employees or links to non-enterprise assets for collaborative purposes.

- **Security Information and Event Management (SIEM) System**: The SIEM system gathers security-related information for subsequent analysis. This data is used to refine policies and issue warnings about potential attacks on enterprise assets.

[36] ibid

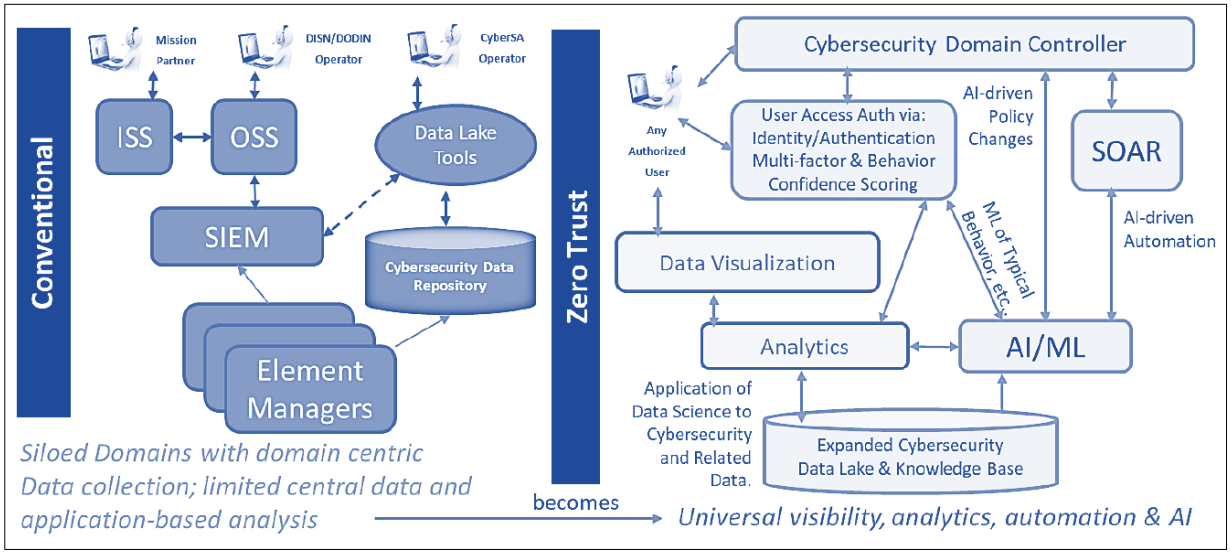
A. Selected Cases of ZTA

Zero Trust (ZT) necessitates a phased adoption of capabilities, technological solutions, process modifications, and the formulation of policies[37]. It's important to note that ZT isn't a one-size-fits-all architectural solution; instead, it is tailored to align with the unique requirements of each organization. Every environment possesses distinct prerequisites, organizational structures, and security policies either already established or in the process of being developed. The subsequent use cases have been crafted with full recognition of this diversity.

1. *Big Data Analytics and Artificial Intelligence (AI)*

In traditional architectures, isolated domains are the norm, and they pose security risks due to inconsistent policies, data, logs, and analytics. These discrepancies create significant challenges because it becomes extremely difficult to gather consistent and comprehensive data that can be effectively analysed and integrated into coherent and dynamic data structures. Each isolated domain contains a portion of the data, such as device security or user login location at a specific point in time. This fragmented data across various isolated domains hampers the speedy analysis of information, necessitating manual efforts to consolidate it into more extensive, relevant datasets. As shown in Figure 5, Zero Trust (ZT) seeks to render isolated domains obsolete by leveraging data analytics and artificial intelligence (AI) to establish a systematic data collection framework[38].

Figure 5. Zero-Trust Framework for Big Data Analytics and Artificial Intelligence



Source: United States of America. Department of Defence, 2022.

This framework can identify data types, establish correlations between datasets, and uncover knowledge or actionable insights through language processing. The incorporation of Big Data further enables the automation of various data preparation tasks, including data gathering, data discovery and assessment, data cleaning and structuring, data transformation and enrichment, and ultimately data publishing and storage. For ZT, this signifies the ability to implement consistent policies, maintain uniform data standards, log information consistently, and employ unified analytics. This, in turn, significantly bolsters the effectiveness of threat detection and mitigation throughout the architecture.

[37] United States of America. Department of Defence, 2022.

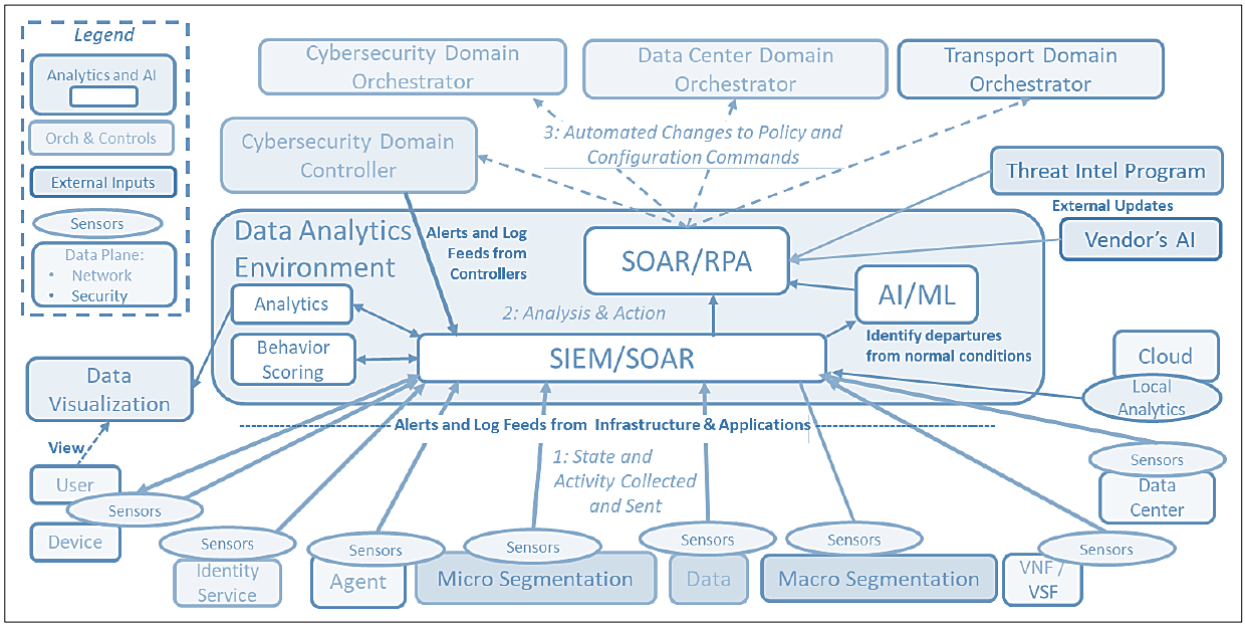
[38] Ibid.

2. *Data Analytics and Artificial Intelligence*

The incorporation of Big Data Analytics and Artificial Intelligence (AI) within the context of Zero Trust (ZT) significantly amplifies the level of visibility, insight, and automation within the environment. Data is systematically gathered from all facets of the environment and subsequently subjected to analysis. In a ZT model, the volume of data collected surpasses that of traditional architectures, primarily due to the data requirements for powering automation. Consequently, more sophisticated tools are necessary to handle this substantial data load.

As shown in Figure 6, Sensors are responsible for collecting data from various components of the environment, transmitting it to a Security Information and Event Management (SIEM) system where it undergoes initial processing and scrutiny to identify potential threats and anomalies. Data pertaining to threats and anomalies, once processed by the SIEM, is then relayed to a Security Orchestration, Automation, and Response (SOAR) system for further analysis, which is bolstered by the involvement of AI. Once threats are confirmed, the ZT controller initiates automated mitigation measures[39]. This information is duly recorded and stored for future Machine Learning (ML) and AI applications, encompassing tasks like User/Network Peripheral Equipment (NPE) confidence scoring, advanced threat identification, the creation and modification of baselines, and collaboration with external intelligence programs and other AI entities to facilitate automation and orchestration. As a component of the ZT architecture, the integration of Big Data Analytics and AI significantly elevates the security posture of modern environments through comprehensive data collection, advanced analysis, and automated threat mitigation.

Figure 6. System Interface Description for Zero-Trust Framework Implementation for Big Data Analytics and Artificial Intelligence



Source: United States of America. Department of Defence, 2022.

[39] Ibid.

V. RECOMMENDATIONS

Drawing upon the background research and the discussion above, a set of recommendations is provided for government agencies and policymakers to guide the successful adoption of emerging technologies and the cultivation of trust within the digital public service landscape. These recommendations are drawn from best practices, case studies, and the principles outlined in this paper.

A. Recommendation 1: Invest on robust and resilient IT Infrastructure

Governments should invest in a secure and robust IT infrastructure that can support digital services without frequent downtime or performance issues, as well as ensure Service Continuity by developing disaster recovery and business continuity plans to ensure that digital public services remain accessible in emergencies and unforeseen events.

B. Recommendation 2: Digital Identity Solutions

Governments should implement secure and user-friendly digital identity solutions. These can help verify the identity of users in a trusted and efficient manner while protecting their personal information and to instil a higher level of trust in online interactions.

C. Recommendation 3: Prioritize Citizen-Centric Design

Government entities should prioritize citizen-centric design principles in the development of digital public services. This includes ensuring user-friendliness, accessibility, and responsiveness to citizen needs. Public sector bodies should engage citizens in the design process, seeking feedback and iteratively improving services. The rationale behind these recommendations is that (i) citizen satisfaction and trust are closely linked to the quality of the user experience, and (ii) involving citizens in the design process ensures that services meet their expectations and requirements.

D. Recommendation 4: Embrace Robust Data Privacy and Protection Measures

Government entities must establish robust data privacy and protection measures to safeguard citizen information. This includes compliance with relevant data protection regulations, encryption of sensitive data, and a commitment to transparency about data practices. The rationale behind these recommendations is that (i) data privacy is a fundamental right, and violations erode trust in government services, and (ii) data breaches can result in significant reputational damage and legal consequences.

E. Recommendation 5: Implement Zero-Trust Architecture

Government entities should consider implementing Zero-Trust Architecture (ZTA) to enhance cybersecurity. ZTA's principles of continuous verification, least privilege, and micro-segmentation reduce the attack surface and mitigate cyber threats effectively. The rationale behind this recommendation is that (i) cybersecurity is paramount in a digital environment, ZTA is a modern approach to protect against evolving threats, and (ii) ZTA enhances data security and ensures trust in the confidentiality of sensitive government information.

F. Recommendation 6: Foster Ethical Use of Technology

Government entities should prioritize the ethical use of technology in public services. This includes addressing bias in algorithms, ensuring transparency in decision-making processes, and adhering to ethical guidelines in emerging technology adoption. The rationale behind this recommendation is that (i) ethical concerns, such as bias and discrimination, can erode trust and lead to negative societal consequences, and (ii) ethical use of technology reinforces trust in government entities' commitment to fairness and responsible behaviour.

G. Recommendation 7: Invest in Digital Literacy and Education

Government entities should invest in digital literacy and education programs for citizens and government employees. Promoting digital literacy enhances responsible technology use, mitigates risks, and fosters trust in digital interactions. The rationale behind this recommendation is that (i) digital literacy empowers citizens to engage effectively with digital services while protecting themselves online, and (ii) skilled government employees are better equipped to handle emerging technologies responsibly.

H. Recommendation 8: Encourage Cross-Sector Collaboration

Government entities should foster collaborative partnerships with industry, academia, and civil society to drive innovation, share best practices, and address emerging challenges. Cross-sector collaboration enhances the exchange of knowledge and promotes responsible technology adoption. The rationale behind this recommendation is that (i) collaboration leverages diverse expertise and resources to navigate complex technological landscapes, and (ii) shared insights and best practices contribute to building trust within the ecosystem.

I. Recommendation 9: Commit to Continuous Improvement

Government entities must commit to continuous improvement in their digital public service offerings. The digital landscape is ever evolving, and entities should adapt to changing technologies, citizen expectations, and emerging threats. The rationale behind this recommendation is that (i) continuous improvement ensures that services remain relevant, secure, and aligned with citizen needs, and (ii) it demonstrates a commitment to providing high-quality, trustworthy services.

These recommendations will serve as a roadmap for government entities and policymakers to navigate the future of digital public services successfully. By prioritizing citizen-centric design, data privacy, cybersecurity, ethical technology use, digital literacy, collaboration, and continuous improvement, agencies can build and maintain trust with citizens and stakeholders while harnessing the benefits of emerging technologies.

VI. CONCLUSION

In an increasingly digital world, the delivery of public services is undergoing a profound transformation. Emerging technologies, such as artificial intelligence, blockchain, immersive technologies, quantum computing, and geospatial technologies, offer unprecedented opportunities to enhance efficiency, responsiveness, and citizen engagement. However, they also bring forth complex challenges related to trust, security, and ethical use. Throughout this paper, we have explored the dynamic landscape of emerging technologies and their roles in shaping the future of digital public services. We have underscored the importance of trust as a cornerstone of effective government-citizen relationships and have emphasized the need for responsible adoption, security, and ethical considerations in leveraging these technologies.

As governments attempt to navigate the evolving digital landscape, it is imperative that they remain committed to the principles outlined in this paper and consider the above recommendations. Trust, security, responsible adoption, and ethical considerations should guide decision-making at every turn. By prioritizing these principles, government entities can build and maintain the trust of citizens and stakeholders, ensuring that emerging technologies are harnessed to enhance the quality, accessibility, and responsiveness of public services. In doing so, they will not only shape a better future for digital public services but also foster a stronger bond of trust between the government and the people it serves.

Bibliography

Bertrand, A. and others (2020). *Artificial Intelligence in the Public Sector: European Outlook for 2020 and Beyond*. Ernst & Young. Available from https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-eBook-artificial-SRGCM3835.pdf.

Global Forest Watch (n.d.). *Forest Monitoring Designed for Action.* Available: https://www.globalforestwatch.org/.

Global Times (2023). *China achieves mobile network algorithm verification powered by quantum computer*. 11 July. Available from https://www.globaltimes.cn/page/202307/1294131.shtml

Kerasidou C. and others (2022). Before and beyond trust: reliance in medical AI. *Journal of Medical Ethics*, Nr. 48, Pp. 852-856.

Lopez, J. (2022). *New plans to slash red tape from 5G roll out and improve mobile phone connectivity*. 25 May. Department for Digital, Culture, Media & Sport. Available from https://www.gov.uk/government/news/new-plans-to-slash-red-tape-from-5g-roll-out-and-improve-mobile-phone-connectivity.

McKnight, D.H. and others (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems*, vol. 11, Nr. 3-4, Pp. 297-323.

Norway. Ministry of Local Government and Modernisation (2019). *One digital public sector: Digital strategy for the public sector 2019-2025*. Available from https://www.regjeringen.no/contentassets/db9bf2bf10594ab88a470db40da0d10f/en-gb/pdfs/digital_strategy.pdf.

Rousseau, D.M. and others (1998). Not so different after all: a cross-discipline view of trust. *Academy of Management Review*, vol. 23, Nr. 3, Pp. 393-404.

TIM Group (2020). *TIM is the first operator in Europe to use quantum computing live on its mobile networks (4.5G and 5G)*. 25 February. Available from https://www.gruppotim.it/en/press-archive/corporate/2020/TIM-Quantum-computing-250220.html.

UNDP and Group of Twenty Presidency (2023). *Accelerating the SDGs Through Digital Public Infrastructure: a Compendium of the Potential of Digital Public Infrastructure.* August. Available from https://www.undp.org/publications/accelerating-sdgs-through-digital-public-infrastructure-compendium-potential-digital-public-infrastructure.

United States of America. Department of Defence (2022). *Zero Trust Reference Architecture: Version 2.0*. July. Available from https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

Veen, M. and others (2011). Emergent technologies against the background of everyday life: discursive psychology as a technology assessment tool. *Public Understanding of Science*, vol. 20, Nr. 6, Pp. 810-825.

WFP (2022). *PRISM: Combining remote sensing and vulnerability data for risk and impact analytics*. 16 November. Available from https://innovation.wfp.org/project/prism.

World Bank (2020). *GovTech: The New Frontier in Digital Government Transformation*. November. Available from https://thedocs.worldbank.org/en/doc/805211612215188198-0090022021/original/GovTechGuidanceNote1TheFrontier.pdf.

World Bank (©2023). *GovTech: Putting People First*. Available form https://www.worldbank.org/en/programs/govtech/priority-themes.