TENSORGATE JOURNAL OF SUSTAINABLE TECHNOLOGY AND INFRASTRUCTURE FOR DEVELOPING COUNTRIES

PRIVACY AND CYBERSECURITY CONCERNS IN SMART GOVERNANCE SYSTEMS IN DEVELOPING COUNTRIES

Joan Telo
https://orcid.org/0009-0004-5101-8064

Abstract

The emergence of smart governance in developing countries has the potential to transform government operations, but it also raises significant concerns about privacy and cybersecurity. A study was conducted to identify specific privacy and cybersecurity concerns in the context of smart governance in developing countries. The findings indicate that data collection and storage are major privacy concerns, as smart governance systems rely on large amounts of personal information, which could be misused for purposes such as surveillance or profiling. Data security is also a significant concern, as developing countries may lack adequate cybersecurity infrastructure, leaving their systems vulnerable to cyber attacks and data breaches. In addition, the lack of data protection laws in many developing countries creates a risk that citizens' data could be mishandled without legal recourse. Citizens may also lack control over their data and not fully understand how it is being collected, used, and shared. Smart governance systems may also be prone to discriminatory outcomes due to biased algorithms, which could violate the privacy rights of marginalized groups. The study also identified significant cybersecurity concerns, including weak cybersecurity infrastructure, insider threats, third-party risks, cybercrime, and political risks. Developing countries may lack the resources and expertise to implement strong cybersecurity measures, leaving them vulnerable to cyber attacks. Trusted insiders may misuse their access privileges, and third-party vendors may have weaker cybersecurity practices, exposing government systems to additional risk. Cybercrime is a significant threat, and smart governance systems may become targets for political attacks, which could compromise the integrity of government systems and undermine public trust in government institutions. The findings of this study highlight the importance of addressing privacy and cybersecurity concerns in the development of smart governance systems in developing countries. It is essential to implement strong data protection laws, invest in cybersecurity infrastructure, and prioritize cybersecurity training and awareness for government employees. Additionally, regular risk assessments and audits should be conducted, and clear protocols and procedures should be established for responding to cybersecurity incidents. International cooperation and information sharing can also help to improve cybersecurity capabilities and respond effectively to cyber threat.

Keywords: Cybersecurity concerns, Data collection, Data security, Developing countries, Privacy concerns, Smart governance

Introduction

Smart governance is a new concept in the field of public administration that emphasizes the use of technology to enhance the efficiency, effectiveness, and transparency of government operations. Smart governance integrates various components of governance such as policy formulation, service delivery, public participation, and data analysis into a single, coherent system. This article discusses the concept of smart governance, its components, advantages, challenges, and best practices.

Smart governance is a modern approach to governance that focuses on leveraging the power of technology to improve governance processes. It involves the use of technology to improve the efficiency and effectiveness of government operations, to enhance transparency and accountability, and to facilitate citizen participation. The goal of smart governance is to create a more responsive, citizen-centered, and efficient government.

The concept of smart governance has its roots in the e-government movement that emerged in the late 1990s. E-government refers to the use of technology to deliver government services to citizens. However, e-government focused mainly on the use of technology for service delivery and did not fully integrate other components of governance such as policy formulation and public participation. Smart governance takes the e-government concept a step further by integrating all aspects of governance into a single, unified system.

The components of smart governance include policy formulation, service delivery, public participation, and data analysis. Policy formulation involves the use of data and analytics to develop policies that are evidence-based and targeted to meet the needs of citizens. Service delivery involves the use of technology to provide citizens with access to government services through digital channels. Public participation involves the use of technology to engage citizens in the decision-making process and to gather feedback on government services. Data analysis involves the use of technology to analyze and interpret data to inform policy decisions and to measure the effectiveness of government services.

Figure 1. Smart governance components in emerging countries

Smart governance has been gaining popularity in developed countries over the past few decades, and now it is starting to take root in developing countries as well. Developing countries face unique challenges when it comes to implementing smart governance, including limited resources, poor infrastructure, and low levels of digital literacy among citizens. This article discusses the challenges and opportunities of smart governance in developing countries and provides examples of best practices. Developing countries are increasingly recognizing the benefits of smart governance. In many cases, these countries are leapfrogging traditional models of governance and moving straight to smart governance. This is because smart governance can

help to overcome some of the challenges that developing countries face, such as limited resources, poor infrastructure, and low levels of digital literacy.

In many developing countries, public services are inefficient and ineffective, resulting in long wait times, low quality, and high levels of corruption. Smart governance can help to streamline service delivery, reduce corruption, and improve the quality of public services. Second, smart governance can help to increase transparency and accountability. In many developing countries, corruption is a major problem that undermines public trust in government. By increasing transparency and accountability, smart governance can help to reduce corruption and improve public trust in government. Third, smart governance can help to promote citizen participation. In many developing countries, citizens feel disconnected from government and do not have a voice in decision-making processes. Smart governance can help to engage citizens in the decision-making process and provide them with a platform to voice their opinions and concerns. Fourth, smart governance can help to promote economic growth. In many developing countries, economic growth is hindered by inefficient government processes, corruption, and limited access to public services. Smart governance can help to create a more efficient and effective government, which can promote economic growth and development.

Privacy concerns for smart governance in developing countries

Data collection and storage

The collection and storage of data are essential components of smart governance systems. Smart governance relies on the use of technology to manage public services and make data-driven decisions. This requires collecting and analyzing large amounts of data, including personal information about individuals. While this data can be used to improve services and enhance decision-making, there is also a risk that it could be used for purposes beyond the original intent. One of the primary concerns with data collection and storage is the potential for surveillance. The use of technology to monitor individuals' behavior and movements can be seen as an invasion of privacy. This is particularly true when the data is collected without individuals' knowledge or consent. It can also lead to abuses of power, such as tracking political dissidents or targeting minority groups. To avoid these risks, it is essential to have strict regulations in place to govern data collection and storage practices. Another concern with data collection and storage is the potential for profiling. When data is analyzed, it can reveal patterns and trends that may be used to create profiles of individuals. These profiles can be used to make decisions about an individual's access to services, employment opportunities, or even their freedom. This is particularly concerning when the data is used to make decisions about marginalized groups or those with limited access to power. It is important to ensure that data is collected and analyzed in a way that is fair and transparent and that individuals have the right to challenge decisions made based on their data.

Data breaches are another concern with data collection and storage. When large amounts of personal information are stored in a single location, it becomes a tempting target for hackers. This can result in sensitive information being exposed, such as medical records, financial information, or even passwords. This can lead to identity theft or other forms of fraud, which can have serious consequences for individuals. To avoid these risks, it is essential to have strong data security measures in place, such as encryption and multi-factor authentication.

Ethical considerations are also important when it comes to data collection and storage. While data can be used to improve services and enhance decision-making, it is essential to ensure that the data is collected and analyzed in a way that is fair and ethical. This means respecting individuals' privacy rights, ensuring that data is collected and analyzed in a transparent manner, and using data for purposes that are consistent with its original intent. It also means being transparent about how data

is being used and ensuring that individuals have the right to access and control their own data. Finally, the long-term storage of data raises concerns about data obsolescence. As technology evolves, data can become outdated and difficult to access. This can make it challenging to use the data for future decision-making or research purposes. It is important to have strategies in place for managing data over the long term, such as regular data backups, migration to new storage systems, or even digitizing physical records.

Smart governance solutions rely heavily on data collection and storage. They do, however, raise privacy, surveillance, profiling, data breaches, ethical concerns, and data obsolescence concerns. To mitigate these dangers, robust laws governing data collecting and storage practices are required. It is also critical to guarantee that data is collected and processed in an open and ethical manner, and that individuals have access to and control over their own data. By addressing these issues, we can ensure that data is used to improve services and make better decisions while protecting people's rights and privacy.

Data security

Data security is a significant concern for all nations, particularly for developing countries that may not have the same level of cybersecurity infrastructure as developed countries. Due to a lack of proper cybersecurity measures, these nations may become vulnerable to cyber-attacks, data breaches, and other cyber threats that could lead to sensitive data being stolen or leaked, compromising the privacy of their citizens. One of the primary reasons why developing countries may be at risk of cyber threats is that they often lack the necessary resources and expertise to implement robust cybersecurity measures. Cybersecurity infrastructure requires significant investment, including the deployment of advanced technologies, hiring trained professionals, and implementing proper policies and protocols. Developing countries may not have the financial resources to invest in such measures, making them more susceptible to cyber-attacks.

Additionally, developing countries may also face challenges in terms of a lack of awareness and knowledge about cyber threats. Many citizens and businesses in these nations may not fully understand the risks associated with cyber threats, making them more vulnerable to phishing, malware, and other cyber-attacks. Lack of awareness and education can lead to careless behaviors such as using weak passwords, clicking on suspicious links, or sharing sensitive data online. Another factor that contributes to the vulnerability of developing countries to cyber-attacks is the rapid pace of technological change. Many developing nations are still in the process of building their technological infrastructure, which makes them more prone to security lapses. As they adopt new technologies and systems, they may not be fully aware of the risks associated with these technologies, making them more susceptible to cyber-attacks.

Moreover, developing countries may also be targets for cybercriminals due to their less stringent data protection laws. Criminals may target these countries for data theft, knowing that they may be less likely to face legal consequences. This creates a vicious cycle where data breaches and cyber-attacks in developing countries become more frequent and severe, leading to further damage to their cybersecurity infrastructure. To overcome these problems, developing countries must invest in cybersecurity infrastructure and foster a culture of cyber awareness and education. This necessitates a substantial investment in new technologies as well as the hiring of experienced personnel to deploy cybersecurity measures. In addition, developing countries should prioritize cybersecurity policies and regulations, enforcing rigorous data protection laws, and establishing effective cybercrime prevention measures. Data security is a significant concern for developing countries due to their less advanced cybersecurity infrastructure, lack of awareness and education about cyber threats, rapid pace of technological change, and less stringent data protection laws. These nations must take proactive steps to strengthen their cybersecurity infrastructure, invest in advanced technologies, hire qualified professionals, and prioritize cybersecurity policies and

regulations. By doing so, developing countries can protect their citizens' privacy and security and contribute to the global effort to combat cyber threats.

Lack of data protection laws

One of the significant challenges that developing countries face in the digital age is the lack of strong data protection laws. Unlike developed countries, many of these nations do not have adequate legal frameworks in place to regulate the collection, use, and sharing of personal information. This lack of regulation creates a significant risk that citizens' data could be misused or mishandled without any legal recourse.

Without strong data protection laws, citizens in developing countries may have little control over how their personal data is collected, processed, and used by governments and private entities. This creates an environment of uncertainty and insecurity, where citizens' privacy and data security are not adequately protected. This lack of protection could lead to personal information being misused, leading to identity theft, financial fraud, and other criminal activities. Moreover, the lack of strong data protection laws in developing countries could also impact international data flows. Companies operating in these nations may not be required to follow the same data protection standards as those in developed countries, creating an uneven playing field. This lack of regulation could make developing countries attractive locations for companies seeking to avoid stricter data protection requirements, leading to further exploitation of citizens' data. Additionally, the lack of strong data protection laws in developing countries could also lead to a digital divide, where citizens in these nations are excluded from participating in the digital economy due to concerns over data privacy and security. This could lead to missed opportunities for economic growth and development, as well as social exclusion and inequality.

To solve these problems, developing countries must prioritize the creation and implementation of stringent data privacy legislation. Significant investment in legal and regulatory frameworks, as well as education and training for government officials and other stakeholders, is required. Collaboration with international organizations is also required in order to promote best practices and standards for data protection and privacy. The lack of strong data protection laws in developing countries poses a significant risk to citizens' privacy and data security. Without adequate legal frameworks in place, citizens may have little control over how their personal data is collected, processed, and used. Developing countries must prioritize the development and implementation of strong data protection laws to ensure that citizens' privacy and data security are adequately protected, and to promote the growth and development of their digital economies.

Consent and control

One of the challenges associated with smart governance systems is the issue of consent and control. Citizens in developing countries may not have adequate control over their data or fully understand how it is being collected, used, and shared by these systems. This lack of understanding and control can lead to a breach of trust between citizens and their governments, which can have negative implications for the effectiveness and legitimacy of these systems. In many cases, citizens may not be aware that their data is being collected or used by smart governance systems. They may not have given their informed consent for the use of their data, or they may not have been informed about how their data will be used. This lack of transparency and communication can lead to a breakdown in trust between citizens and their governments, which can undermine the effectiveness of smart governance systems.

Moreover, citizens may not have adequate control over their data, which can create a sense of powerlessness and lack of agency. They may not have the ability to opt-out of data collection, or they may not be able to access or delete their data. This lack of control can leave citizens feeling vulnerable and exposed, which can further erode trust in smart governance systems.

To resolve these concerns, governments must prioritize transparency and communication in their use of smart governance systems. Citizens must be informed about how their data will be collected, used, and shared, and they must be given the ability to give informed consent or opt-out of data collection. Governments must also prioritize the development of mechanisms for citizens to access and control their data, such as data protection rights and privacy-enhancing technologies. In addition, civil society organizations and the media must play a critical role in holding governments accountable for their use of smart governance systems. They must ensure that citizens are informed and aware of the risks associated with these systems, and they must advocate for greater transparency and control over the use of citizen data.

The issue of consent and control is a significant challenge for the effective implementation of smart governance systems in developing countries. Citizens must be informed and empowered to control how their data is collected, used, and shared by these systems. Governments must prioritize transparency and communication, and civil society organizations and the media must play a critical role in holding governments accountable for their use of citizen data. Only by addressing these challenges can smart governance systems be effectively implemented to benefit citizens and promote development in developing countries.

Discrimination and bias

Smart governance systems rely heavily on algorithms and machine learning to process and analyze large amounts of data. While these technologies can improve decision-making and increase efficiency, they can also perpetuate discrimination and bias if not carefully designed and monitored. This is a significant challenge associated with the implementation of smart governance systems in developing countries. One of the main concerns is that algorithms may be trained on biased data, which can result in discriminatory outcomes. For example, an algorithm used to predict criminal behavior may be trained on data that over-represents certain demographics or criminal offenses, resulting in unfair treatment and the violation of privacy rights of marginalized groups. This type of bias can perpetuate existing inequalities and exacerbate discrimination in society. Another issue is that algorithms may be designed with implicit biases, reflecting the values and assumptions of their developers. This can result in algorithms that are not neutral or objective, but rather reflect and perpetuate existing biases and stereotypes. For instance, a facial recognition system designed to identify individuals may not be as effective in recognizing individuals with darker skin tones, which can result in discriminatory outcomes and privacy violations for marginalized groups.

It is critical to give the creation of impartial and fair algorithms top priority in order to overcome these issues. This necessitates a multidisciplinary strategy with many viewpoints and specialties. In order to detect and fix biases that may develop over time, algorithms also need to be continually monitored and evaluated. Moreover, governments must prioritize the protection of privacy and the rights of marginalized groups in their use of smart governance systems. This includes ensuring that algorithms are transparent, and decisions are explainable and justifiable. Citizens must be informed about how these systems work, how their data will be used, and how decisions will be made.

In addition, civil society organizations and the media must play a critical role in monitoring and evaluating the use of smart governance systems. They must ensure that these systems are not perpetuating discrimination or violating privacy rights and advocate for greater transparency and accountability in the development and implementation of these systems. The issue of discrimination and bias is a significant challenge for the implementation of smart governance systems in developing countries. It is crucial to prioritize the development of unbiased and fair algorithms, protect privacy and the rights of marginalized groups, and ensure transparency and accountability in the use of these systems. Only by addressing these challenges can smart governance systems be effectively implemented to promote development and social justice in developing countries.

Cybersecurity concerns for smart governance in developing countries

Weak cybersecurity infrastructure

Developing countries often struggle with weak cybersecurity infrastructure, which can leave them vulnerable to cyber attacks. These attacks can result in the theft of sensitive data, financial loss, and damage to critical infrastructure. The lack of resources and expertise to implement strong cybersecurity measures is a significant challenge for many developing countries. One of the main problems is weak passwords, which can make it easy for hackers to gain access to systems and data. Many users in developing countries use simple and easy-to-guess passwords, such as "123456" or "password." This can make it easy for hackers to crack passwords and gain access to systems and data. Another issue is unpatched systems. Many developing countries may not have the resources or expertise to keep their systems up to date with the latest security patches. This can leave them vulnerable to known vulnerabilities that can be exploited by hackers.

The lack of encryption is also a significant problem in developing countries. Encryption is an essential security measure that can protect data from unauthorized access. However, many systems in developing countries may not have encryption enabled or may use weak encryption, leaving data vulnerable to interception and theft. Prioritizing the creation of robust cybersecurity infrastructure in developing nations is essential for addressing these issues. Strong security measures, such as the use of strong passwords, frequent system updates, and the usage of encryption, must be used in order to achieve this. The development of rules and regulations that encourage the deployment of robust security measures and the protection of crucial infrastructure is another requirement for governments to emphasize cybersecurity as a national security concern. Public-private partnerships can also be successful in enhancing cybersecurity infrastructure in poor nations, since private businesses can support government initiatives with resources and knowledge.

In addition, awareness-raising campaigns can be effective in promoting good cybersecurity practices among the general public. This includes educating users about the importance of using strong passwords, keeping systems up to date, and enabling encryption. Weak cybersecurity infrastructure is a significant challenge for many developing countries, leaving them vulnerable to cyber attacks. It is crucial to prioritize the development of strong cybersecurity measures, including the use of strong passwords, regular system updates, and encryption. Governments, private companies, and civil society organizations must work together to improve cybersecurity infrastructure in developing countries and promote good cybersecurity practices. Only by addressing these challenges can developing countries effectively protect their citizens' data and critical infrastructure from cyber threats.

Insider threats

Insider threats are a significant concern for smart governance systems, as they rely on trusted insiders to access and manage sensitive data. These insiders can include employees, contractors, and third-party vendors who have been granted access privileges to the system. However, insiders may intentionally or unintentionally misuse their access privileges, leading to data breaches and other cybersecurity incidents.

Intentional insider threats occur when an insider deliberately misuses their access privileges to steal sensitive data, damage systems, or disrupt operations. This can include theft of intellectual property, financial fraud, or sabotage. In some cases, insiders may be motivated by personal gain, such as financial rewards, or by ideological or political motives. Unintentional insider threats, on the other hand, occur when an insider accidentally or unknowingly causes a security incident. This can include actions such as opening a phishing email, using weak passwords, or falling for a social engineering attack. These actions can lead to data breaches or other cybersecurity incidents that compromise the integrity, confidentiality, and availability of sensitive data.

Smart governance systems must employ robust security measures to avoid, identify, and respond to insider incidents in order to address insider threats. This includes implementing access controls to limit insiders' access privileges, using monitoring technologies to detect odd or suspicious behavior, and implementing incident response plans to respond rapidly to security incidents. Access controls should be implemented to ensure that insiders only have access to the data and systems necessary to perform their job duties. This can include the use of role-based access controls, which limit access based on the user's job function, and the implementation of two-factor authentication, which adds an extra layer of security to user login credentials. Monitoring tools can help detect unusual or suspicious behavior by insiders, such as accessing data outside of their job duties or accessing data at unusual times. These tools can also monitor for unauthorized data exfiltration or system changes that may indicate an insider threat.

Incident response plans should be developed and regularly tested to ensure that organizations can quickly respond to insider threats. This includes procedures for investigating and mitigating incidents, as well as communication plans to notify stakeholders and the public about the incident. Insider threats are a significant concern for smart governance systems, as they rely on trusted insiders to access and manage sensitive data. Smart governance systems must employ robust security measures to prevent, detect, and respond to insider incidents in order to address insider threats. This includes implementing access controls, monitoring instruments, and incident response plans. By taking these measures, intelligent governance systems can better secure their sensitive data and prevent insider-caused cybersecurity incidents.

Third-party risks

Smart governance systems may rely on third-party vendors for technology and support, such as cloud hosting, software development, or maintenance services. These vendors may have weaker cybersecurity practices than the government, exposing the government's systems to additional risk. This is particularly concerning if the vendor has access to sensitive data or systems that are critical to the functioning of the smart governance system. Third-party risks can come from a variety of sources, including inadequate security controls, weak passwords, or unpatched software. Vendors may also be targeted by attackers seeking to gain access to the government's systems through a vulnerable third-party connection.

Smart governance systems must thoroughly vet and monitor their third-party vendors to address third-party risks. This includes conducting security audits of the vendor's systems and processes, as well as checking their contracts to ensure they satisfy security standards. Smart governance systems must also ensure that their vendors use secure software development practices, such as code review processes, vulnerability testing, and secure coding standards. This can help prevent software vulnerabilities from being exploited by attackers. Furthermore, smart governance systems must require vendors to provide strong access controls, such as two-factor authentication and access monitoring, to prevent unwanted access to government systems. Smart governance systems must also establish incident response plans that take third-party risks into consideration. This comprises protocols for investigating and mitigating security incidents that may have been caused by a third-party link, as well as communication plans for informing stakeholders and the general public about the occurrence. Finally, smart governance systems must verify that third-party providers follow data protection rules and regulations. This covers data processing and storage regulations, as well as reporting and notification procedures in the event of a data breach.

Third-party risks are a significant concern for smart governance systems, as they rely on third-party vendors for technology and support. To address these risks, smart governance systems must carefully vet and monitor their third-party vendors, ensure they are using secure software development practices and strong access controls, and develop incident response plans that account

for third-party risks. By taking these steps, smart governance systems can better protect their sensitive data and prevent cybersecurity incidents caused by third-party connections.

Cybercrime

Developing countries may be more vulnerable to cybercrime, including phishing attacks, ransomware, and other forms of malware. This is due to a variety of factors, such as weak cybersecurity infrastructure, lack of cybersecurity awareness, and limited resources for cybersecurity investments. Phishing attacks, for example, can trick government employees into giving away their login credentials or other sensitive information. Ransomware can encrypt government data, making it inaccessible until a ransom is paid. Other types of malwares can compromise the integrity of government systems or steal sensitive data. Cybercrime can have serious consequences for smart governance systems. It can compromise the confidentiality, integrity, and availability of government data and systems, leading to loss of trust and credibility. It can also result in financial losses due to the cost of investigating and mitigating the incident, as well as potential legal liabilities.

Smart governance systems must make investments in robust cybersecurity measures, like as firewalls, intrusion detection and prevention systems, and malware protection software, to handle the issue of cybercrime. In order to aid government employees in identifying and averting typical cyberthreats like phishing attacks, they also need to offer cybersecurity training and awareness initiatives. To make sure they are ready to detect and react to cyber incidents in a timely and effective manner, smart governance systems must also create and test incident response strategies. Procedures for isolating infected systems, recovering data from backups, and informing stakeholders and the public about the event are all included in this. In order to exchange threat intelligence and coordinate responses to cybercrime, smart governance systems must collaborate with law enforcement organizations and other partners. This can help strengthen the nation's overall cybersecurity posture and help stop cybercriminals from effectively attacking government networks. Last but not least, in order to prevent cybersecurity issues, advanced governance systems should examine and update its safeguards on a regular basis. This entails performing security checks, such as vulnerability scans, penetration tests, and update and patch installations, on a regular basis. Intelligent government systems in low-income countries face serious cyberthreats. Smart governance systems must invest heavily in cybersecurity measures, provide cybersecurity training and awareness programs for government employees, create and test incident response plans, collaborate with law enforcement and other partners, and review and update cybersecurity measures on a regular basis in order to address this threat. These measures will help ensure that smart governance systems' sensitive data and systems are safe from cybercriminals.

Political risks

Smart governance systems are vulnerable to political risks that can undermine their effectiveness and legitimacy. One such risk is political attacks, which can take various forms, including hacktivism, state-sponsored cyber espionage, and other forms of cyberattacks aimed at disrupting or undermining government operations.Hacktivism is the use of hacking techniques to promote a political agenda or social cause. Hacktivists may target government systems to expose corruption or human rights abuses, or to protest government policies. These attacks can disrupt government operations and compromise the confidentiality and integrity of government data.

State-sponsored cyber espionage, on the other hand, involves the use of cyberattacks by one country against another for political or military gain. Governments may use cyber espionage to steal sensitive information, disrupt critical infrastructure, or undermine the stability of another country. Political attacks on smart governance systems can have serious consequences. They can compromise the integrity of government systems and undermine public trust in government

institutions. They can also lead to the theft or loss of sensitive government data, compromising national security or other critical operations. To address political risks, smart governance systems must invest in strong cybersecurity measures, including firewalls, intrusion detection and prevention systems, and malware protection software. They must also develop and test incident response plans, to ensure they are prepared to detect and respond to cyber incidents in a timely and effective manner. In addition, smart governance systems must engage with law enforcement agencies and other partners to share threat intelligence and coordinate responses to political attacks. This can help prevent state-sponsored cyber espionage and other forms of political attacks, and can improve the overall cybersecurity posture of the country.

To increase public trust and lessen the likelihood of political attacks, smart governance systems should emphasize openness and accountability in all aspects of their work. Among these are providing transparent and clear communication to the public about government operations and policies, regularly auditing and reviewing government systems, and enforcing robust data protection laws and regulations. Finally, sophisticated administrative structures should be ready to counteract the effects of political assaults. Critical activities must have backup and recovery procedures in place, and the government must be able to effectively communicate with stakeholders and the public about the disaster and its reaction. Smart governance systems are especially vulnerable to political risks in underdeveloped nations. Smart governance systems that want to counteract this risk should implement robust cybersecurity safeguards, collaborate with law enforcement and other partners, encourage openness and accountability, and be ready to respond to and lessen the effects of political attacks. Smart governance systems can better safeguard sensitive data and systems from political threats by adopting these measures.

Conclusion

The adoption of smart governance systems in developing countries has the potential to enhance efficiency, transparency, and accountability in government operations. However, this increased digitization also comes with privacy and cybersecurity concerns, which if not addressed adequately, can lead to serious consequences. These concerns may arise due to the lack of adequate infrastructure, funding, and technical expertise, which are common challenges faced by developing countries.

Smart governance systems may collect, store, and use large amounts of personal data, such as citizens' biometric information, financial records, and social media activities. This data may be vulnerable to misuse, such as identity theft, profiling, and surveillance, which can have severe consequences for individuals' privacy and security. Furthermore, citizens may be reluctant to engage with smart governance systems if they perceive their privacy is at risk. One solution to address privacy concerns is to ensure that smart governance systems are compliant with privacy laws and regulations. Developing countries can adopt a comprehensive data protection framework that outlines the legal requirements for data collection, storage, use, and disclosure. The framework should also establish a data protection authority responsible for enforcing privacy laws and providing guidance on data protection practices.

Another solution is to implement privacy-enhancing technologies (PETs) in smart governance systems. PETs are designed to protect personal data by minimizing the collection of identifiable information, ensuring data security and confidentiality, and providing individuals with greater control over their data. For example, smart governance systems can use encryption, anonymization, and pseudonymization techniques to protect personal data. Additionally, individuals can be provided with access and control over their data, including the right to delete their data and revoke consent for its use. Smart governance systems are vulnerable to cybersecurity threats such as

hacking, malware attacks, and data breaches. Cybersecurity threats can result in the loss of sensitive information, financial losses, and damage to the reputation of government institutions. Furthermore, cyber threats can lead to disruptions in government operations and services, which can affect citizens' trust in the government.

Developing countries can assess their cybersecurity risks and establish appropriate measures to manage and mitigate these risks. Incident response plans should be in place to identify and respond to cyber threats effectively. Additionally, awareness-raising activities can educate government employees and citizens about cybersecurity risks and how to protect against them. It is important to ensure that smart governance systems are designed with cybersecurity in mind. This means adopting a secure-by-design approach, where cybersecurity considerations are integrated into the development process from the outset. Security features such as firewalls, intrusion detection systems, and antivirus software should be incorporated into smart governance systems to protect against cyber threats. Additionally, regular security audits and vulnerability assessments should be conducted to identify and address any security weaknesses in the system.

Developing countries may lack the technical expertise and funding required to develop and implement secure smart governance systems. One solution is to invest in capacity building initiatives that equip government employees with the necessary technical skills and knowledge to develop and manage smart governance systems. These initiatives can include training programs, workshops, and mentoring schemes that focus on cybersecurity and privacy best practices.

Collaboration between government institutions, private sector actors, and civil society organizations can also play a critical role in addressing privacy and cybersecurity concerns in smart governance systems. Partnerships can enable the sharing of resources, expertise, and best practices, which can lead to more effective and sustainable solutions. Collaboration can also facilitate the development of innovative solutions that meet the specific needs and challenges of developing countries. It is essential to ensure that privacy and cybersecurity are not overlooked in the rush to digitize government operations. Governments in developing countries must prioritize these issues and invest in the necessary resources to address them. Failure to do so can have severe consequences for citizens' privacy and security, as well as government operations and services. Ultimately, the success of smart governance systems in developing countries will depend on their ability to balance the potential benefits with the need for privacy and cybersecurity safeguards.

References

[1] S. Alawadhi and H. J. Scholl, “Smart governance: A cross-case analysis of smart city initiatives,” *2016 49th Hawaii international*, 2016.

[2] M. do Rosário Matos Bernardo, “Smart City Governance: From E-Government to Smart Governance,” in *Smart Cities and Smart Spaces: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2019, pp. 196–232.

[3] M. N. I. Sarker, M. Wu, and M. A. Hossin, “Smart governance through bigdata: Digital transformation of public agencies,” in *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 2018, pp. 62–70.

[4] F. Anindra, S. H. Supangkat, and R. R. Kosala, “Smart Governance as Smart City Critical Success Factor (Case in 15 Cities in Indonesia),” in *2018 International Conference on ICT for Smart Society (ICISS)*, 2018, pp. 1–6.

[5] H. J. Scholl and S. AlAwadhi, “Smart governance as key to multi-jurisdictional smart city initiatives: The case of the eCityGov Alliance,” *Soc. Sci. Inf.* , vol. 55, no. 2, pp. 255–277, Jun. 2016.

[6] S. Barns, “Smart cities and urban data platforms: Designing interfaces for smart governance,” *City, culture and society*, 2018.

[7] H. J. Scholl and S. AlAwadhi, “Creating Smart Governance: The key to radical ICT overhaul at the City of Munich,” *Inf. Polity*, vol. 21, no. 1, pp. 21–42, Feb. 2016.
[8] A. Herdiyanti, P. S. Hapsari, and T. D. Susanto, “Modelling the Smart Governance Performance to Support Smart City Program in Indonesia,” *Procedia Comput. Sci.*, vol. 161, pp. 367–377, Jan. 2019.
[9] D. Mutiara, S. Yuniarti, and B. Pratama, “Smart governance for smart city,” *IOP Conf. Ser.: Earth Environ. Sci.*, vol. 126, no. 1, p. 012073, Mar. 2018.
[10] S. Goldsmith and S. Crawford, *The responsive city: Engaging communities through data-smart governance*. John Wiley & Sons, 2014.
[11] W. Cellary, “Smart governance for smart industries,” in *Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance*, Seoul, Republic of Korea, 2013, pp. 91–93.
[12] Z. Tomor, A. Meijer, A. Michels, and S. Geertman, “Smart Governance For Sustainable Cities: Findings from a Systematic Literature Review,” *Journal of Urban Technology*, vol. 26, no. 4, pp. 3–27, Oct. 2019.
[13] H. Willke, “Smart governance: governing the global knowledge society,” 2007.
[14] E. W. Johnston and D. J. Hansen, “Design lessons for smart governance infrastructure,” in *Transforming American governance: Rebooting the public square*, Routledge, 2015, pp. 209–224.
[15] M. Razaghi and M. Finger, “Smart Governance for Smart Cities,” *Proc. IEEE*, vol. 106, no. 4, pp. 680–689, Apr. 2018.
[16] M. P. R. Bolívar and A. J. Meijer, “Smart Governance: Using a Literature Review and Empirical Analysis to Build a Research Model,” *Soc. Sci. Comput. Rev.*, vol. 34, no. 6, pp. 673–692, Dec. 2016.
[17] H. J. Scholl and M. C. Scholl, “Smart governance: A roadmap for research and practice,” in *iConference 2014 Proceedings*, 2014.
[18] J. Mooij, “SMART GOVERNANCE?,” 2003.
[19] N. V. Lopes, “Smart governance: A key factor for smart cities implementation,” in *2017 IEEE International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2017, pp. 277–282.
[20] G. V. Pereira, P. Parycek, and E. Falco, “Smart governance in the context of smart cities: A literature review,” *Information Polity*, 2018.
[21] C. Liu and J. Huang, “DDoS Defense Systems in Large Enterprises: A Comprehensive Review of Adoption, Challenges, and Strategies,” *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 2, no. 1, pp. 1–21, 2018.
[22] N. Ní Loideain, “Cape Town as a smart and safe city: implications for governance and data privacy,” *International Data Privacy Law*, 2017.
[23] L. F. M. Ramos and J. M. C. Silva, “Privacy and Data Protection Concerns Regarding the Use of Blockchains in Smart Cities,” in *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance*, Melbourne, VIC, Australia, 2019, pp. 342–347.
[24] A. Martinez-Balleste, P. A. Perez-martinez, and A. Solanas, “The pursuit of citizens’ privacy: a privacy-aware smart city is possible,” *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 136–141, Jun. 2013.
[25] M. Witti and D. Konstantas, “A Secure and Privacy-preserving Internet of Things Framework for Smart City,” in *Proceedings of the 6th International Conference on Information Technology: IoT and Smart City*, Hong Kong, Hong Kong, 2018, pp. 145–150.
[26] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, “Security and Privacy in Smart Cities: Challenges and Opportunities,” *IEEE Access*, vol. 6, pp. 46134–46145, 2018.
[27] L. Yang, N. Elisa, and N. Eliot, “Chapter 7 - Privacy and Security Aspects of E-Government in Smart Cities,” in *Smart Cities Cybersecurity and Privacy*, D. B. Rawat and K. Z. Ghafoor, Eds. Elsevier, 2019, pp. 89–102.
[28] A. Verma, A. Khanna, A. Agrawal, A. Darwish, and A. E. Hassanien, “Security and Privacy in Smart City Applications and Services: Opportunities and Challenges,” in *Cybersecurity and*

Secure Information Systems: Challenges and Solutions in Smart Environments, A. E. Hassanien and M. Elhoseny, Eds. Cham: Springer International Publishing, 2019, pp. 1–15.

[29] L. van Zoonen, "Privacy concerns in smart cities," *Gov. Inf. Q.*, vol. 33, no. 3, pp. 472–480, Jul. 2016.