

**National College of Ireland**

**Project Submission Sheet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name:** | Ansh Ashwini Jain / Jagadish Babu Sake / Rohit Kumar Veluguri / Sai Venkat Prem Mummalaneni / Yamini Madupathi | | |
| **Student ID:** | 23308320 / 23310341 / 23232510 / 23297191 / 23234750 | | |
| **Programme:** | MSc in Cyber Security | **Year:** | 2024 |
| **Module:** | Data Governance, Ethics, Sustainability | | |
| **Lecturer:** | Mr. Joel Aleburu | | |
| **Submission Due Date:** | 8th November 2024 | | |
| **Project Title:** | A Pathway to Sustainable Smart Cities: Ethical Approaches to Global Challenges | | |
| **Word Count:** | 5984 | | |

**I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.**

**ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.**

|  |  |
| --- | --- |
| **Signature:** | Ansh Ashwini Jain / Jagadish Babu Sake / Rohit Kumar Veluguri / Sai Venkat Prem Mummalaneni / Yamini Madupathi |
| **Date:** | 8th November 2024 |

**PLEASE READ THE FOLLOWING INSTRUCTIONS:**

1. Please attach a completed copy of this sheet to each project (including multiple copies).

2. Projects should be submitted to your Programme Coordinator.

3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.

4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**

5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

|  |  |
| --- | --- |
| **Office Use Only** | |
| Signature: |  |
| Date: |  |
| Penalty Applied (if applicable): |  |

A PATHWAY TO SUSTAINABLE SMART CITIES: ETHICAL APPROACHES TO GLOBAL CHALLENGES

Ansh Ashwini Jain  
Masters of Science in Cybersecurity  
National College of IrelandDublin, Ireland  
x23308320@student.ncirl.ie

Sai Venkat Prem Mummalaneni  
Masters of Science in Cybersecurity  
National College of IrelandDublin, Ireland  
x23297191@student.ncirl.ie Jagadish Babu Sake  
Masters of Science in Cybersecurity  
National College of IrelandDublin, Ireland  
x23310341@student.ncirl.ie

Yamini Madupathi  
Masters of Science in Cybersecurity  
National College of IrelandDublin, Ireland  
x23234750@student.ncirl.ie Rohit Kumar Veluguri  
Masters of Science in Cybersecurity  
National College of IrelandDublin, Ireland  
x23232510@student.ncirl.ie

***Abstract***-**The Atlanta ransomware attack in March 2018 underscored how vulnerable city systems can be to cyber threats. The hackers were able to take down Atlanta’s digital infrastructure in March, and this caused residents have faced many problems- especially in aspects like utility bill payment and court case handling. In totality, it brought to face some of the challenges of today's urban areas. It is a reminder that with every new technology we embrace, we must take a moment and change our communities for the better- make sure people can trust their city systems.**

***Keywords- Governance, Ethics, Atlanta, Smart City***

1. *INTRODUCTION*

Within our Connected World, Data Management Shall Become Far More Critical to Keeping Safe and Fair Use. Ransomware hit Atlanta, Georgia, in 2018. The Attack Gain showed vulnerability in the context of a larger question raised in the way cities manage data and cybersecurity with too many connected devices. As cities infuse more technology, the ethical question of data collection, storage, and usage will have to be raised. Strengthening rules to protect sensitive information and uphold ethical standards in all communities was the clarion call that came from the Atlanta Incident. City leadership must address cybersecurity not just for the exigency but must prepare the city for further assaults [7].

When we discuss data management, ethics, and sustainability, it reminds us that cybersecurity isn't just a separate issue; it’s part of a bigger plan to keep people safe and maintain their trust. This means using technology responsibly and making sure the public feels secure in city systems. The lessons from the Atlanta attack are key to shaping better policies in the future. As we embrace smart technology, we also need to commit to ethical and sustainable data practices.

The problem is a ransomware attack on Atlanta that occurred in March 2018, exposed vulnerabilities of such a magnitude in the information systems of the city and caused major disruptions to the delivery of critical services by crippling several city departments and, in turn, the ability of residents to pay utility bills and access court records. This incident is an example of how critical strong cybersecurity and efficient data management are becoming as cities put more trust in technology.

It is indeed very important that this issue is addressed for a few key reasons. First, the attack created significant problems for residents as it made it difficult for them to access important services and clearly showcased just how much cyber threats can disrupt everyday life. The city had to spend over $2.7 million on the recovery, money which could have gone to other important services or towards fixing infrastructure. Finally, incidents like this erode people's trust in local government, especially when sensitive information is compromised, and services are disrupted. This much stronger cybersecurity measures.

1. *SDG FOCUS*

Improving cybersecurity measures include the following major objectives as priorities. Initially, the city’s IT systems should be fortified against potential future attacks and enhanced readiness to combat any cyber threats. Secondly, abreast of best practices in cybersecurity, knowledge among city employees would help in eliminating mistakes that could cause problems. Thirdly and lastly, clear data protection and incident handling policies shall ensure all parties are aware of their responsibilities in case of an issue.

The Atlanta attack underscores the major aspects involved in making better cities. Goals emphasized by SDG 11: Sustainable Cities and Communities, focusing on adequate infrastructure and cybersecurity to ensure the safety and sustainability of urban areas. On the one hand, SDG 16: Peace, Justice, and Strong Institutions underline a high degree of significance in the effectiveness with which city leaders govern. This is building, and keeping the trust of the public while ensuring that city services are secure and safe and reliable particularly when dealing with cyber threats.

The attack on Atlanta pointed out serious vulnerabilities in the city’s IT systems, which means that they must be more regularly checked and updated to stay secure. Because of that attack, for weeks many important city services were shut down. This forced employees to go back to doing things by hand which is much less efficient. The decision not to pay the ransom meant that the recovery took a long time, in turn highlighting how important it is to have a clear plan for dealing with these kinds of situations in the future [8].

1. *GOVERNANCE FRAMEWORKS*

The tech applied to urban management is how smart cities develop, where sustainability and efficiency come from taking decisions based on data. The paper reveals the weakness of such systems, as seen in the ransomware attack on Atlanta in 2018, which led to a review of governance and regulatory frameworks of how data is used in urban contexts.

1. *Local Government Regulations*

Local authorities are tasked with creating rules concerning data management and cybersecurity within their areas. In Atlanta, officials responded to the ransomware attack by strengthening cybersecurity measures, updating policies, and implementing new data protection protocols. This included a comprehensive Cybersecurity Strategy focusing on risk management and incident response.

1. *Federal Guidelines*

The federal government establishes guiding frameworks, like the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework aids municipalities in risk management and cyber incident response, promoting structured governance of data.

1. *Data Protection Laws*

Regulations like GDPR in Europe and CCPA in the U.S. dictate standards for personal data handling. These laws, while not universally applicable, set a precedent for best practices in data security and privacy, encouraging municipalities to implement stringent data protection measures.

1. *International Agreements*

Global frameworks influence local data handling practices, pushing jurisdictions towards stricter compliance and enhanced data governance standards.

1. *Cybersecurity Regulations*

Entities such as the FTC and CISA set rules governing municipal cybersecurity practices, aimed at safeguarding critical infrastructure from cyber threats.

1. *Sustainability Standards*

Organizations like the Global Reporting Initiative (GRI) promote sustainability standards in data governance, urging municipalities to align data practices with environmental and sustainability goals.

1. *Ethical Data Use Guidelines*

Ethical frameworks emphasize transparency, accountability, and fairness in data management, guiding cities in making ethical decisions regarding data collection and utilization.

1. *Interagency Collaboration*

The Atlanta incident underscored the need for partnerships between local and federal entities to enhance cybersecurity posture, requiring effective communication among stakeholders.

1. *Regulatory Compliance*

Local governments must comply with data protection regulations to avoid legal repercussions and maintain public trust, as highlighted by the Atlanta ransomware attack [9].

1. *ETHICAL CONSIDERATION*

Incidents such as the Atlanta ransomware attack raise by orders of magnitude the level of importance for proper governance that considers data privacy and equity concerns in the wake of such ethical dilemmas. The governance framework should therefore cover not only protection and privacy over how data is handled but also how the solution results from data serve all segments of the community to drive down the technological divide. Ethical governance requires sturdy cybersecurity to protect against breaches. More so, there should be transparency; citizens have a right to know how their data is managed and the risks involved. Local governments should assume their responsibility by accounting for their cybersecurity actions and making sure residents have given informed consent about the use of their details. In addition, the adoption of only-that-is-required data minimization reduces breaches. Resilience and recovery strategies, though should be within governance integration, allow cities to bounce back from crises with minimal disruption in service. The securities of interconnected infrastructures, more specifically IoT devices, should be done to preclude vulnerabilities. Public trust may, however, be attained through proper data ethics that will cement community support for smart city initiatives.

1. *DATA PROTECTION*

To ensure safety and inclusivity for cities and environments considering the public in picture, a lot of measures need to be taken to guarantee sustainability and urban development. Following are a few measures which can be followed to greaten the strength between developing an urban city with moralities that enhance data privacy and create transparency.

1. *GDPR PRINCIPLES*

Considered to be one of the toughest security and privacy law in the world, Global Data Privacy Protection (GDPR) is a framework which provides with set guidelines to collect and process information of the public present in the European Union (EU) [1]. It is now even considered as a global benchmark for protection of data as it allows to emphasize on transparency, user content and right to privacy. There are multiple principles and roles that can be applied with the current goal of enhancing security in communities, few of them are as following:

1. *Data Minimization*

In a scenario, where there are huge chunks of data which is collected, like traffic data, banks, municipalities as suggested, there are high chances of data misinterpretation. Chances of data not being used for what they are actually meant to be for are high, and for exactly this scenario, we need to ensure proper protocols are in place to minimize the data usage, and limited to the scenario at hand.

1. *Purpose Limitation*

Similarly, the purpose for data usage needs to be clear from start, as in such scenarios, they should only be present for the specific scenario at hand, like data used to improve traffic flow should not be used to collect samples of license plate images for issue speculations.

1. *User Consent and Control*

The strongest framework for GDPR is the User Consent and control as it emphasizes on the authority the user has. The user needs to have complete access control and needs to know also understand as to what happens with their data. This ensures their right over their data, the right to access it, modify it when required and even delete it when needed.

1. *Accountability*

Considering municipalities and larger organizations at play here, they should take the role of responsibility to clear the rules and regulations in force to protect their customer’s data, which increases the trust in the residents. In case of any breach or mishap, responsible actor needs to be held accountable for the actions.

1. *Lawfulness, fairness and transparency*

This principle states that any processing of data needs to be legally done, keeping rules and regulations in hand by lawfully abiding to them and ensuring fairness to all. The area needs to be transparent about from where the personal data is collected, used, consulted or otherwise used and till what level will it be used [2].

1. *BENEFITS OF GDPR*

Following are a few ways which we propose as to how principles mentioned above can help out in ensuring that GDPR is complying with the Sustainable development Goal 11 with the benefits in doing so:

1. *CCTV and Surveillance*

Most of the recent urban cities now use surveillance cameras to monitor crimes and ensure safety for betterment of the society. Purpose Limitation and User Consent and control are certain GDPR policies which can be used and applied here by using techniques like keeping the user anonymous and letting their residents know how their surveillance data will be used to ensure the trust stays maintained.

1. *Personal Data Protection*

As earlier mentioned in the Atlanta City Attack, because of certain access being lost and coming in hands of unauthorized users, there was loss of online payment data and court records. All of this being sensitive information which was not accurately and safely stored which caused disruptions for residents on unfathomable levels. This can be avoided with applying policies from GDPR by ensuring the accountability of the data the organizations hold and the consent of the user to access the data is being maintained and tracked [3].

1. *Data Maintenance*

Considering a smart city, there are loads and loads of data present at hand. Traffic information, air quality, energy usage, personal records etc. With so much data at hand to handle and ensure protection, GDPR needs to be applied to ensure the right usage of the data. For example, a certain resident’s traffic data needs to be collected only to understand overall traffic in general and not the specific location in which the user is travelling. This ensures it’s only for the stated purpose and then once it’s processed it’s no longer needed to be used.

1. *Law Regulation*

The greatest and the most required principle is of the law regulation, where in a smart city, the principle of lawfulness in GDPR is applied. The data collected needs to be fairly processed by law and correctly measured and used keeping rules set by the city. There should be no illegal processing on any data and the treatment needs to be equal for one and all.

1. *GDPR CHALLENGES*

Following are a few challenges which can be met while trying to comply GDPR in the most accurate way for any urban city development.

1. *Balancing Transparency*

Transparency in any format states that without de-railing from the originated use of the function, how to ensure everything is accurately applied and created. In a municipality or a smart city, ensuring transparency while applying GDPR protocol is the highest necessity for all of the users present. The greatest challenge is in the private sector as there can be certain rules and regulations which need to be thoroughly followed and maintained with clear communication between agreed parties. Also, as GDPR focuses on citizen engagement, striking a balance between how the data can be used, and how it should be exactly used can be a challenge as between rights and public information required for the betterment of the city, the initiative can slow down transparency efforts.

1. *IOT Device Data*

Keeping the vastness at hand, there are multiple IOT devices at hand which is being used to ensure that a city becomes a smart city. With the need of making a city smart, comes in multiple devices which are at risk of a data breach or a misuse if not acted or treated correctly. This can pose as a problem if the safeguarding as set by GDPR is not accurately followed. Encryption of data being transferred and proper storage is a must necessary for this protocol. Clear consent of user and their need to know as to what the data is being used for is also in picture with the GDPR as a requirement. As there can be multiple third-party vendors, chances of transparency, data ownership and control can be shared across many parties. If the clarity of usage is not clear, it can create a lack of trust in the citizens which can cause a backlash [4].

1. *DATA-DRIVEN TECHNOLOGIES*

By Using the different data-driven technologies, like a smart city initiative, will help achieving some sustainable goals by promoting their efficient resource management and developing the service delivery. more-ever, these implications of the latest technologies must be critically analyzed to make sure of the usage of ethical and legal compliance and social equity.

1. *ETHICAL IMPLICATIONS*

Ethical Implications represents the potential outcomes or results that appear from different actions, decisions, and some main policies, specifically on moral principles. In the different contexts, this ethical implication includes how the choices will impact on any individuals or communities, and society, pointing on this problem like a fairness, justice, accountability, and mainly all the rights for the those who affected. And they will verify how will these different actions aligning with moral values and principles standards [12].

1. *Public Trust*

They are some cyber security threats which can destroy public’s trust on government institutions. So this atlanta attack shows how the government were failed to protect the personal data of every citizen’s may which leads to skepticism which shows the ability of the government of protecting data’s

1. *Data Privacy and Security*

This attack will raise remarkable questions on the responsibility of municipal government to protect their citizen information. Ethical concerns raised when it considering as an acceptable cities of cyber security prevention measures before only to safeguard their various constituents if not it can lead to huge data breaches of people’s personal information

1. *Transparency and Accountability*

With the help of public resources on the stake, choosing accountability for attacks are vital. This Ethical implication combines the transparency for communicating about impact on various attacks and responses for. mainly to ethical governance which only needs pure transparency on how the data was collecting and how it’s using and how was it protecting. This implication involves the need of process for decision making which are related to cyber security on investments and practices of data governance

1. *The Cost to Citizens*

mainly it focusses on process of recovering the financial burden and so many fell on taxpayers. So, the Ethical considerations will appear regards to management of public financial funds and the adequacy of preparedness for cyber attacks

1. Privacy Concerns

By using the data-driven technologies often includes the data collection of peoples personal information. This Atlanta attack explains the risks of getting data breaches, where it can compromise sensitive information. and Ethical considerations regards on the collection and protecting personal information are paramount.

1. Responsibility and Accountability

these Ethical implications include the main responsibility of every organization to have safeguarding cyber security. In this attack of Atlanta incident, some of the questions are raised about the city's structure against on cyber-attack threats and accountability of those who are in position of leadership are the failures to protect the data.

1. *Balancing the Innovation and Security*

The activity of innovation in the public services by delivery through some of the data-driven technologies which are need to be balanced against on the robust of various security measures. Ethical dilemmas will lead up when the organizations prioritize, they’re some of the technological advancement without any properly addressing the potential of vulnerabilities in the cyber security.

1. *Ethical Usage of Data*

The ethical usage of sensitive data which involves in making sure of every citizen in all the consent, and by maintaining some transparency among people in society about data collecting and data using, and protecting individual personal data privacy.

1. *LEGAL IMPLICATIONS*

Some of the Legal Implications will refer to potential effects on different actions, or any decisions, or any situations under the purview of law. These implications will take a positive or negative forms which can play a significant role in controlling the legal responsibilities of any individuals or any organizations were connected with particular context. and these Legal implications are more important across all different areas, including contractual agreements, regulatory compliance of unlawful activities. And understanding all the rules and regulation of legal standards [10].

1. Compliance with Some Regulations

This attack is highlighted with potential and non-compliance with the help of data protecting regulations, using the needs for municipalities to get legal frameworks and that government data must be more security and privacy, like GDPR (General Data Protection Regulation) for entities operating dealing with citizens of EU’s

1. Liability for Data Breaches

So, the Local governments may face some of legal issues for failing to protect people’s data correctly. This may lead to regulatory actions if it is determined that negligence contributed to the data breach.

1. Policy Development

This attack was discussed about importance of strong policies of cyber security at municipal levels, and also includes immediate incident response plans and also some risk management factors and strategies of legal standards.

1. Regulatory of Frameworks

Adequately this cyber-attack was developed by some of the law makers by the aiming to implement stronger regulations on cyber security for government which has recreant the perfect framework to the government and shows the how the people will able to handle their data securely.

1. Legal Compliance:

As the municipalities to adopt more and more advanced data-driven technologies, so that they can be comply with the existing of some laws and future new regulations to get sure that they will protect people’s sensitive data or information adequately.

1. *SOCIAL IMPLICATIONS*

It refer to main effects of some actions, and policies have on any individuals and communities. They are some implications which enclosed a huge range of outcomes, which includes the changes in some social values, behaviors, and economic conditions. By Understanding the social implications is much important for checking how the different initiatives will impact on the social fabric and overall well-being of citizens. These implications will enclose the ways which are social structures, and relationships and some values will be influenced by the specific changes [11].

1. Public Confidence and Trust

This ransomware attack will major impacted on public’s trust in city ability to protect the information of citizens and deliver some essential services. They are some social implications which involves the potential of long-term trust on government institutions, which can be affected by citizen participation in the city activities.

1. Community of Resilience

This attack revealed the main vulnerabilities in any city's infrastructure, mainly they need a social resilience in any cyber threats face. and the Communities must be educated about various risks which are associated with the data-driven technologies and encouraged to participate in the discussions on the data governance and also on cyber security.

1. Impact on Smart City services Initiatives

As cities are rapidly increasing Ing to adopt the latest smart technologies to improve the urban governance, then the attack will raise on the social implications of which is depending on the systems of data-driven. Some of the issues like a surveillance and data ownership, the usage of ethical technology should be addressed to make sure that smart city initiatives have to implement in some random way that should be benefits to all the citizens.

1. Digital Divide

These are some implications of ransomware attacks may be highly affects the vulnerable in the populations, this lack of service access to alternative some services, like a bigger or economically disadvantages which may be a specific impacted when the public services are been interrupted.

1. Equity and Access

Some of the Vulnerabilities in the digital infrastructure which can majorly affects some implemented guidelines of communities which may already having the only limited access for the technology and to services. Make sure to equitable access to get a secured digital service is more important for the justice for social. Some citizens who are deeply affected they are mainly from lower income people in the society who are mainly rely on the municipal services in society

1. Community Engagement

This incident will define the importance of connecting with all communities about the risks of cyber security and which have to be in a protective measure. Mainly by conducting public people awareness campaigns in every city can help to more people in educating the residents on protecting their personal data or sensitive information and recognizing potential threats.

1. Social Inclusion

By Implementing some of the data-driven solutions which can strive to including some of the ensuring all the various community members in a team which can benefit for all advanced technological to advancements without any existing in the inequalities.

Using data-driven technologies, such as smart city initiatives, can help achieve sustainable goals by promoting efficient resource management and improving service delivery. However, the implications of these technologies must be critically analyzed to ensure ethical use, legal compliance, and social equity.

1. *SUSTAINABILITY MATTERS*

In today rapid changing technological advancement population are migrating from the rural area to urban spaces. For their Job opportunities and for the quality of life with world class amenities. They are willing to rely on and adopt to smart technologies for living, transportation, entertainment, medical care. Which in turn generates enormous amount of data that need to be handle carefully by imposing the data governance, policies & ethic and cybersecurity norms. They consecutively become a solid pillar for the sustainable cities. It is purely data driven cities also known as “Smart cities”.

Everything comes at a price. With this high-tech advancement comes with high cyber security risks and data protection and storge complications. So, need to follow the ethical framework, good data handling practices and policies to gain public trust and urban resilience.

Data Governance in sustainable cities: In our smart city point of view which include people, process and technologies. It is necessary to follow DAMA-DMBOK framework for the data governance by establishing policies, procedures and standard norms which allows the city authorities to collect, filter, store, analyses and protect vast amount of data from diverse sources like Govt. administrative office, post office, transportation services which enhances decision making [5].

Key aspects of Data Governance in smart cities:

* Extensive Data policies: Creating crystal clear policies crafted precisely for requirements across the domains, implementing strict access rules and taking into consideration compliance in data protection laws across local and international boundaries.
* Data Ownership and custodianship: City Authorities should have a strict principle in data processing life cycle. It is very critical for the further analysis of data and in making decisions. Each and everything have to be documented where the data originated from, who owns the data and data management, accountability. City Authorities should have assigned teams to handle such things, can outsource to data stewards or third parties.
* Data Quality: Data that has been collected from various sources should be reliable and consistent. To maintain sustainability the data should undergo various protocols and standards must be compatible among the various departments and technologies for accurate decision making.
* Data privacy and security: This should be our main priority to protect the data by implementing various cybersecurity technics for End-to-End encryption by using cipher or encryption algorithms for storage, usage of TLS channel for data transmission, using strong multifactor authentication to accessing the systems and proper security audits should be carried out on regular intervals.
* Compliance with Legal and regulatory requirements: Cities should follow the strict compliance practice and systematic methodologies (like GDPR, HIPPA) to avoid the legal issues to safeguard the public data. Which will ensure citizens trust and hope [6].

Challenges in Data Governance:

* Limited Funding and resources: Most of the cities lacks in insufficient financial and human resources to implement the data governance frameworks, lack of monitoring system. Lack of awareness in employee and the public on the cyber threats.
* Enormous Data: Huge amount of data is generated by the cities from various sources. It is a big challenge in itself to segregate, process and store data, which requires an advanced technology and infrastructure to run this smoothly we need the skill professional.
* Stakeholders and partnership: The cities hold huge number of stakeholders like government agencies, private organisations, NGO’s and citizens which makes it difficult to manage and monitor the data governance practices, by maintaining balance and transparency among them.

Ethical Implications in sustainable city development: Ethics play a major role in data governance for sustainable cities, to make sure that the technologies used are easily access and available to the public, maintaining privacy stands. The governance mainly focusses on constant innovation with data privacy, public safety and trust.

1. *ETHICAL PRINCIPLES*

* Transparency and accountability: All the organisations and data management firms must be transparent about the entire Data cycle process. So that citizens should access data at any point time promoting the data availability and accountability.
* Rationality and social Equality: It is most important thing that digital literacy should be implemented uniformly across all the domains, not limiting to certain groups or individuals. Ensuring that it should promote equal benefits and unbiased data collection and processing across the sustainable city to maintain the social harmony.

Example: Free public Wi-Fi to connect to online services, transportation etc.,

* Privacy and Autonomy: The cities authorities must respect individuals right to privacy by securing data and permitting individuals control over their personal information, they need to provide option to hide out unnecessary data collections across the city.

Ethical challenges:

* Ethical collection of data for the safety and environmental monitoring considering the public privacy rights can be challenging.

Example: CCTV surveillance in sensitive places and private area without the public consent.

* Providing the smart city resources is not always easy and evenly distributed. Due to the lack of population and less density area like outside the city limits. City authorities need to make a clear margin for it.

1. *CORE STRATEGIES*

Cybersecurity and sustainable data practices: As the cities rapid expanding, it is prone to the cyber-attacks due to the extensive digital infrastructure and valuable data. Cities needs a highly sophisticated and robust cybersecurity measures.

* Zero Trust Architecture: Operates on the premise that every device and user should be treated as risks, to security measures by enforcing verification and implementing stringent access controls to safeguard sensitive information effectively against unauthorized access.
* Training and awareness: All the employees, data stewards, partners and contractors must be trained to recognize cyber threats, data handling with care and adhere to protocols, being aware of cybersecurity can lower the chances of falling victim, to phishing scams and malware attacks.
* Data Encryption and Anonymization: Following this cybersecurity practice for cities sensitive information, even in case of attack. Data encryption ensures that unauthorized user cannot read the data with the proper encryption key. On the other hand, anonymization prevents the identification of individuals.
* Advanced threat Detection: All the control & command centers and Web services should have advanced threat detection system using the AI and ML to detect and respond to attack. And take a proactive measure to defend the attack.
* Incident response plans: The authorities should have well developed incident response plan to tackle and minimize the damage cause by the attack. Which ultimately help in limiting the disruption to the essential services.

1. *CONCLUSION*

In summary, as urban areas evolve into smart cities, the interplay between governance frameworks, ethical data use, and sustainability objectives becomes crucial in addressing the challenges posed by technological advancements while safeguarding citizens' interests. It is necessary to know which frameworks are implemented to understand how exactly can a city become ‘smart’ without being vulnerable to issues at hand. The mentioned ethical principles and policies are in line with the data-driven solutions can transform the urban habitat into the smart city that focuses on people and plant. Primarily focusing on the data handling techniques, using the AI & ML to make our lives convenient and reducing the usage of paperwork and the physical money in the city administration will meet the needs of present without compromising future.

Most of the futuristic based cities are on their road to implement meaningful technologies like smart banks, computerized court orders and much more. All of these generate vast amount of data. The only way to ensure smoothening of the data collection is by creating a more reliable environment by applying ethical challenges and policies. All of this will help in reducing waste, optimizing energy and improving public services. With pre-defined limits to understand how much data is being actually collected and used, the residents in picture should be aware of how their data is being used. This allows growth in making transparent policies and allows the user to be in control of their own data.

Striking a balance between transparency and GDPR compliance is crucial for smart cities aiming to meet SDG 11. To manage these challenges, cities can implement privacy-centered policies, apply advanced methods for anonymizing data, integrate privacy protections from the outset, and prioritize clear, citizen-focused communication. This strategy helps ensure that smart city projects comply with GDPR while supporting sustainable, trust-building urban development goals.

Our goal is to build the sustainable smart cities connecting all the major principles and policies in the Data governance, ethical challenges and sustainability through the data driven solutions and the latest technologies. In Ethical Data management adopt to transparent, consistent, processing and storing using industrial standard frameworks. From Environmental point we can adopt towards renewable energy sources like solar energy, wind power, hydro power generation and promote the use of EV vehicles create awareness in public mindset. For the data protection using standard cybersecurity protocols, real time threat monitoring and incident response plan. Maintaining balanced ecosystem, equality, citizen privilege rights and good social harmony to promote quality of life.

To be successful in smooth running of the smart cities we need collaboration between city authorities, private sector and citizens. As the cities evolute on time, it important to adopt to new trend and technology, synchronise with ethical practice and frameworks for our future.

*REFERENCES*

1. J. Ladley, *Data governance : how to design, deploy, and sustain an effective data governance program*. Amsterdam: Elsevier/Mk, 2012.
2. S. Sharma, *Data Privacy And Gdpr Handbook.* S.L.: John Wiley & Sons, 2019.
3. S. Earley, *DAMA-DMBOK: Data Management Body of knowledge*, 2nd ed. Basket Ridge, New Jersey: Technics Publications, 2017.
4. Data Protection Commission, “Principles of Data Protection | Data Protection Commission,” *Principles of Data Protection | Data Protection Commission*, 2022. <https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection>
5. R. Neshovski, “Home,” United Nations Sustainable Development. Accessed: Nov. 04, 2024. [Online]. Available: <https://www.un.org/sustainabledevelopment/>
6. “Cybersecurity Framework,” *NIST*, Nov. 2013, Accessed: Nov. 04, 2024. [Online]. Available: <https://www.nist.gov/cyberframework>
7. “Atlanta Ransomware Case Study | Avast Business,” *Avast.ua*, 2018. <https://www.avast.ua/business/resources/atlanta-ransomware#mac> (accessed Nov. 01, 2024).
8. “Atlanta Still Feeling the Effects of Cyberattack | INSUREtrust,” *Insuretrust.com*, 2018. <https://insuretrust.com/2018/05/02/atlanta-still-feeling-the-effects-of-cyberattack/> (accessed Nov. 01, 2024).
9. Nations, “Sustainable cities and human settlements .:. Sustainable Development Knowledge Platform,” *Un.org*, 2015. <https://sustainabledevelopment.un.org/topics/sustainablecities>
10. S. Harvey, “Ransomware Alert: Lessons Learned from the City of Atlanta,” KirkpatrickPrice. Accessed: Nov. 05, 2024. [Online]. Available: <https://kirkpatrickprice.com/blog/ransomware-alert-lessons-learned-city-atlanta/>
11. B. Freed, “One year after Atlanta’s ransomware attack, the city says it’s transforming its technology,” StateScoop, Mar. 22, 2019. <https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/>
12. “SDG 11 - Sustainable cities and communities,” ec.europa.eu. <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=SDG_11_-_Sustainable_cities_and_communities#Sustainable_cities_and_communities_in_the_EU:_overview_and_key_trends>.