SMART 2024

The Thirteenth International Conference on Smart Systems, Devices and Technologies

ISBN: 978-1-68558-151-0

April 14 - 18, 2024

Venice, Italy

SMART 2024 Editors

Lasse Berntzen, University of South-Eastern Norway, Norway

SMART 2024

Forward

The Thirteenth International Conference on Smart Cities, Systems, Devices and Technologies (SMART 2024), held between April 14th and April 18th, 2024, continued a series of international events covering tendencies towards future smart cities, specialized technologies and devices, environmental sensing, energy optimization, pollution control and sociocultural aspects.

Digital societies take rapid developments toward smart environments. More and more social services are digitally available to citizens. The concept of 'smart cities', including all devices, services, technologies, and applications associated with the concept sees a large adoption. Ubiquity and mobility added new dimensions to smart environments. Adoption of smartphones and digital finder maps and increasing budgets for technical support of services to citizens settled a new behavioral paradigm of city inhabitants.

We take here the opportunity to warmly thank all the members of the SMART 2024 technical program committee, as well as all the reviewers. The creation of such a high-quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to SMART 2024. We truly believe that, thanks to all these efforts, the final conference program consisted of top-quality contributions. We also thank the members of the SMART 2024 organizing committee for their help in handling the logistics of this event.

We hope that SMART 2024 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the field of smart cities, systems, devices, and technologies.

SMART 2024 Chairs

SMART 2024 Steering Committee
Lasse Berntzen, University of South-Eastern Norway, Norway
Young-Joo Suh, POSTECH, Korea

SMART 2024 Publicity Chairs
Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain
José Miguel Jiménez, Universitat Politecnica de Valencia, Spain

SMART 2024
Committee

SMART 2024 Steering Committee

Lasse Berntzen, University of South-Eastern Norway, Norway
Young-Joo Suh, POSTECH, Korea

SMART 2024 Publicity Chairs

Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain
José Miguel Jiménez, Universitat Politecnica de Valencia, Spain

SMART 2024 Technical Program Committee

Lounis Adouane, Université de Technologie de Compiègne / Heudisayc, France
Ramakalyan Ayyagari, National Institute of Technology Tiruchirappalli, India
Karolina Baras, University of Madeira, Portugal
Lasse Berntzen, University of South-Eastern Norway, Norway
DeJiu Chen, KTH Royal Institute of Technology, Sweden
Patrizio Dazzi, University of Pisa, Italy
María del Mar Gómez Zamora, Universidad Rey Juan Carlos, Spain
Marta Sylvia del Río, Universidad de Monterrey, Mexico
Daniel Delahaye, ENAC LAB, Toulouse, France
Rachid El Bachtiri, USMBA University, Morocco
Abdelali Elmoufidi, University of Hassan II Casablanca, Morocco
Steffen Fries, Siemens AG, Germany
Marco Furini, University of Modena and Reggio Emilia, Italy
Angelo Furno, LICIT laboratory - University of Gustave Eiffel / University of Lyon, France
Ivan Ganchev, University of Limerick, Ireland / University of Plovdiv "Paisii Hilendarski", Bulgaria
Ilche Georgievski, University of Stuttgart, Germany
Maria Helena Gomes de Almeida Gonçalves Nadais, University of Aveiro, Portugal
Jorge J. Gomez-Sanz, Universidad Complutense de Madrid, Spain
Javier Gozalvez, Universidad Miguel Hernandez de Elche, Spain
Fakhrul Hazman Yusoff, Universiti Teknologi MARA, Malaysia
Gerold Hölzl, University of Passau, Germany
Tzung-Pei Hong, National University of Kaohsiung, Taiwan
Javier Ibanez-Guzman, Renault, France
Sergio Ilarri, University of Zaragoza, Spain
Abdelmajid Khelil, Landshut University of Applied Sciences, Germany
Pinar Kirci, Bursa Uludag University, Turkey
Tshepo Godfrey Kukuni, Central University of Technology, South Africa
Wolfgang Leister, Norsk Regnesentral, Norway
Giovanni Livraga, Universita' degli Studi di Milano, Italy
Giuseppe Mangioni, University of Catania, Italy
Manuel Mastrofini, Università degli studi di Roma Tor Vergata & LAST Horizon, Italy
Kevin Meehan, Atlantic Technological University, Ireland

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Navigating Security Issues of Interoperability in the Digital Identity System of a Smart City 1
Amarilda Koka and Pierre-Martin Tardif

Intelligent Bus Shelter as an Example of the Novel Smart City Technology Integration 8
Tomasz Wejrzanowski, Konrad Owieczko, Lukasz Pulka, and Piotr Wroblewski

Introducing Advanced Comparative Life Cycle Assessment for Evaluating Environmental Conditions and Carbon Opportunity Costs of Energy Production Facilities 10
TaeHyung Kwon, Sunghwan Kim, and Juyeong Maeng

Navigating Security Issues of Interoperability in the Digital Identity System of a Smart City

Amarilda Koka
Université de Sherbrooke, Canada
Université de Bretagne-Sud, France
email: koka1501@usherbrooke.ca

Pierre-Martin Tardif
Université de Sherbrooke, Canada
email: pierre-martin.tardif@usherbrooke.ca

Abstract—As the digital landscape develops, the significance of seamless interoperability in digital identity systems becomes even more apparent. As a part of a smart city, identity management and integrated technology are essential in improving administrative operations and promoting e-government development, bringing services closer to citizens and the local economy. This paper focuses on a Canadian Smart City of just under a million inhabitants, which has to solve crucial issues enabling the right balance between safeguarding user privacy and maintaining effective interoperability between varied platforms. This study explores the barriers to seamless interoperability among various digital identity systems and proposes future work that move toward a secure, user-centric, and inclusive digital identity ecosystem.

Keywords-digital identity; interoperability; Identity Access Management cycle; security risks; Smart Cities.

I. INTRODUCTION

Globalization, information, and the electronic communication revolution are the primary reasons for Smart Cities and governments to orchestrate services and systems in order to revolutionize the way information is used and public goods and services are delivered to citizens. The custom of maintaining several email accounts for diverse purposes has become widespread, while the rapid growth of Internet users, mobile phone users, and email accounts has revolutionized the way people manage their online identities.

In this research, the context is developed using Canadian laws, rules and standards. In this regard, the Digital ID and Authentication Council of Canada (DIACC) has created the Pan-Canadian Trust Framework (PCTF). The PCTF defines a set of auditable processes and guidelines for the creation, management, and use of identity information that ensures the trustworthiness of the identity ecosystem [1]. However, as Canada is a federation, its current identity landscape is divided into various jurisdictions, including the federal state, the provinces, and the territories. For example, the federal government is responsible for employment insurance, immigration, and defense. Among others, Canadian jurisdictions are responsible for driver's licenses, health insurance, and the civil registry. As a result, Canada has no unique identifier available for identification. Although the organizations responsible for each of these silos have made significant efforts to protect their distinct identification systems for their specific needs, none of them were intended to serve as a reliable and all-encompassing identity instrument. Considering that Smart City services must use personal information, the identity management system must minimize data access according to the user profile, whether the person is an employee, works in a government agency or an enterprise, or represents themselves as a citizen [2]. Central to securing access to digital assets and enabling secure interactions with online platforms is the Identity Access Management (IAM) cycle, encompassing identification, authentication, and authorization. The IAM cycle aims to enhance security and productivity while minimizing costs and repetitive tasks, encompassing crucial functions such as user creation, deletion, access granting, and revocation [3].

Identification constitutes the initial and essential step in the IAM cycle, pivotal in verifying user authenticity and facilitating access to resources and services. The authentication phase of the IAM cycle requires users to present an authenticator, typically a password or cryptographic module, to verify their identity. Although various authentication mechanisms exist, including passwords, access cards, and biometric measurements, passwords remain widely used despite their inherent weaknesses. Password reuse and weak choices continue to pose security risks, even with the addition of special characters [4]. In response to these concerns, multi-factor authentication protocols merge different authentication factors, including passwords and supplementary devices like mobile phones or authentication tokens. The final phase, authorization, grants users' access to specific resources, guided by the principles of least privilege and separation of duties. The principle of least privilege advocates granting individuals only the minimum number of authorizations required to perform their duties, thus minimizing the potential damage caused by insider threats. On the other hand, the segregation of duties principle implies that sensitive business functions require the involvement of at least two individuals, thus reducing the likelihood of fraud by requiring collusion between two employees and minimizing the impact of wrong action by one of them.

However, as digital identity management develops, the need for seamless interoperability among different identity systems becomes increasingly critical. This raises numerous security challenges, including secure data exchange, authentication compatibility, data standardization, privacy

 ISBN: 978-1-68558-151-0

and consent management, consistent authorization, vulnerability to security exploits, regulatory compliance, audibility, user education, and technological compatibility. The delicate balance between addressing these security concerns and seamless data exchange requires collaborative efforts, standardization, and robust security measures throughout the IAM cycle.

This research paper delves into the intricate web of security challenges encountered in achieving seamless interoperability within the IAM cycle of digital identity systems. Through an assessment of potential risks and vulnerabilities during information exchange and authentication processes, this study aims to identify key areas of concern that demand rigorous attention and innovative solutions to ensure the integrity, confidentiality, and availability of user data. By addressing these security challenges head-on, this research seeks to pave the way for a resilient, secure, and user-friendly IAM cycle, fostering trust and confidence in today's interconnected digital landscape.

The rest of the paper is organized as follows. Section II provides an analysis of related work done so far for the interoperability of digital identity systems, the background of a Smart City, some of the most common interoperability challenges and opportunities, followed by security issues and challenges. It ends with the analysis of some of the most com- mon attacks on authentication protocols. Section III presents a system model incorporating all the requirements proposed for a Smart City, and Section IV presents a use case as a road map solution for this model. Conclusions and future work are presented in Section V.

II. RELATED WORK

Several studies have explored the complexities of digital identification systems and interoperability within Smart Cities; however, in defining the scope of our related work, we strategically focus on two pivotal studies, with the goal of integrating the current discourse on digital identification and interoperability in Smart Cities. This careful selection serves as a foundation for generalizing previous findings and emphasizes our efforts to expand on current contributions, providing distinctive perspectives and broadening academic research on this topic. Notably, Bonneau et al. [5] provide a comprehensive methodology for identifying and evaluating web authentication systems, with an emphasis on usability. In contrast, our research concentrates on a specific collection of protocols, offering a nuanced security analysis that addresses weaknesses associated with DoS (Denial of Service) and Man- in-the-Middle attacks. Our approach integrates these attacks together with every step of the IAM cycle in a model to provide a thorough study of security issues.

Since blockchain technology has received significant attention in the literature for its potential to improve security, privacy, and trust in Smart Cities, numerous studies have highlighted these factors as main incentives for incorporating blockchain into Smart City applications. Georgiou et al. [6] present research that investigates various forms of blockchain, such as consortium, hybrid, private, and public, and assesses their suitability to the specific needs of Smart Cities. However, it is not the same approach in our research because of the concerns related to acceptability and trust levels, particularly in countries where people are skeptical about depending on a technology with an anonymous origin. The essential anonymity of blockchain raises concerns about the openness and accountability of the digital identity ecosystem. Further- more, uncertainty about the probable failure of blockchain technology in the future influenced the choice.

As we navigate the area of digital identity interoperability, our proposed system model takes a new approach. Unlike earlier research, we anticipate a government-backed intermediary account in Smart Cities to improve user identification and permission processes. This intermediary account, rather than storing or processing user information, makes use of existing frameworks and standards to ensure a secure and privacy focused digital identity ecosystem. Our study represents a step forward in the field of digital identity systems in Smart Cities, providing an achievable path for increased security and efficiency.

A. Background

Smart Cities' interoperable e-government initiatives come with the objective of facilitating better and more efficient delivery of information and services to citizens, promoting productivity among public servants, encouraging the participation of citizens in government, and empowering all citizens through the use of information technologies with the goal of making government more result-oriented, efficient, and citizen-centered.

Ministries and agencies in Smart Cities government create, retain, and archive a variety of fragmented citizen information. For instance, the Department of Public Safety keeps information about a citizen, the Revenue and Tax Authority keeps further information about the same citizen, and the Social Services Department keeps other information about the same citizen. In this way, citizens carry several sorts of identity cards to be identifiable by a specific government agency or public institution, in addition to storing fragmentary information. This brings to light the reason why the government of Smart Cities requires an interoperable digital identity system that handles the long-term initiative of such activities in order to achieve the goals of i) using electronic identity management to improve collaboration between government agencies by reducing duplication of efforts and increasing the efficiency and effectiveness of resource utilization, and ii) reducing transaction costs for the government, citizens, and the private sector by providing products and services electronically.

As the government has dispersed identity information among several public institutions and government agencies, accessing and sharing this data, i.e., interoperability, has become a challenge. Integrating and interfacing with various government agencies and public entities that maintain

 ISBN: 978-1-68558-151-0

fragmented information is also an important problem to address. Furthermore, privacy and security concerns about citizens' identity information must be addressed, and the interchange of this information via secure channels to assure confidentiality and integrity is a serious concern.

B. Broad Interoperability Challenges and Opportunities

In the realm of governmental systems, the concept of interoperability has traditionally been approached from a predominantly technical perspective, focusing on resolving technical challenges and ensuring seamless data exchange. However, a comprehensive understanding of the interoperability problem necessitates an exploration beyond purely technical aspects. In the context of public service, the full scope of interoperability encompasses multifaceted dimensions influenced by diverse sources. Thus, to holistically address the interoperability challenge, it becomes imperative to take into account not only technical factors such as data semantics and process standardization but also an array of nontechnical elements, including legal considerations, political dynamics, and social implications. Embracing this broader perspective will enable more effective solutions and foster efficient collaboration among government entities and services. Starting with the main definitions, we can define interoperability as the ability of Information and Communication Technology (ICT) systems and the business processes they support to exchange data and enable the sharing of information and knowledge [7], and e-government interoperability, in its broad sense, as the ability of constituencies to work together. At a technical level, it is the ability of two or more diverse government information systems or components to meaningfully and seamlessly exchange information and use the information that has been exchanged [8].

In the domain of digital identity interoperability, organizations encounter numerous challenges, particularly with the increasing adoption of cloud and multi-cloud systems. Achieving seamless interoperability is not a straightforward task, and organizations must grapple with interconnected issues. Despite being perceived by residents, businesses, and employees in a Smart City as a single entity, the government necessitates separate interactions with multiple departments and agencies to access services, leading to a lack of communication between jurisdictions and hindering seamless service delivery.

Security also emerges as a critical concern in digital identity systems, with the risk of compromising the integrity of an identity system increasing as more individuals gain access to a particular digital identity. Breaches or leaks pose significant challenges for correction, depending on the protocols and implementation in place. The potential for hackers to impersonate trusted servers further increases security risks, leading to identity theft or the disruption of the entire trust network.

Looking ahead, international challenges in digital identities prompt collaborative efforts between Canada and the European Commission (EC). Both parties embarked on a discovery phase through a joint workshop series to explore digital credentials and identify areas of commonality and gaps to be addressed to enable interoperability and mutual support for digital credentials [9].

Among the major gaps, the absence of standards for digital wallets creates an environment reminiscent of the "wild west" in the market, undermining trust and interoperability potential. Additionally, Zero-Knowledge Proofs (ZKP) emerge as a novel method for communication without sharing personal data. However, before standardization, a comprehensive under- standing of ZKP is imperative to establish relevant policies, including considerations of General Data Protection Regulation (GDPR) compliance and whether ZKP proofs qualify as personal data. Resolving these gaps and challenges will be pivotal in shaping a secure and efficient digital identity interoperability landscape for smart cities.

C. Security Issues and Challenges

In the present-day landscape, the existence of multiple vendors offering diverse options has given rise to a critical challenge in developing identity management systems that prioritize individuals' control over their personal data, described as user-centric digital identity [10]. Ensuring that individuals retain the authority to manage the extent of information collected and disclosed about them becomes paramount. The increasing expansion of identities further compounds the complexities associated with aspects such as proof of ownership, identity-to- holder linkage, attribute transferability, and authorization [11]. Consequently, the design and attributes of the Identity Access Management cycle demand a comprehensive and adaptive approach to address these evolving requirements. However, with the increasing reliance on digital technologies and the rise of sophisticated cyber threats, each step of the IAM cycle faces its own unique set of security challenges. From the vulnerabilities in the identification process that expose individuals to identity theft and impersonation attacks to the risks associated with weak authentication mechanisms and flawed authorization practices, addressing the security challenges within the IAM cycle is critical to safeguarding digital assets and preserving user trust. Three widely adopted Federated Identity Management standards are Security Assertion Markup Language (SAML), Open Authentication (OAuth), and OpenID Connect (OIDC). Among these, the OAuth 2.0 protocol stands out as one of the most extensively used authorization and Single-Sign-On (SSO) protocols. Moreover, it serves as the underlying framework for the emerging SSO standard, OpenID Connect. Despite the widespread adoption of OAuth, previous analysis efforts primarily focused on identifying bugs in particular implementations and were based on formal models that abstracted from various web features or lacked a formal treatment altogether [12].

D. Security Attacks on IAM Technologies

Based on the literature evaluation, we used a targeted method to find substantial research on typical threats against digital identification systems, notably in Smart City scenarios. We initiated our search using established databases such as IEEE Xplore, ACM Digital Library, and

 ISBN: 978-1-68558-151-0

Google Scholar, focusing on criteria related to digital identification security and Smart City application.

The selection procedure supported research that provided information on security vulnerabilities, and attack vectors. These selected papers were critically analyzed to extract essential conclusions relating to security concerns. Some of the most prevalent attacks that can occur in IAM technologies are as follows:

1) 307 Redirect Attack in OAuth: In this security attack, the attacker exploits a vulnerability that compromises the authorization and authentication properties of the system. The attack occurs when the user logs in at an Identity Provider (IdP) that utilizes an incorrect HTTP redirection status code. This simple error in the HTTP redirection process allows the attacker to gain access to the user's credentials during the loginprocedure [13].

2) Man-in-the-Middle (MITM) Attack in SAML: In the context of SAML, one potential vulnerability is observed in the SP-Initiated SSO message flow when utilizing POST and artifact bindings. During this exchange, the user seeks to access a resource on the Service Provider (SP) website, even though they do not possess a valid login session on this site. Instead, their federated identity is managed by the Identity Provider (IdP) (e.g., saml-idp.com) [14].

In this flow, the SP saves the requested resource URL in local state information and sends an HTML form containing a SAML AuthnRequest message to the user's browser via an HTTP response (HTTP status 200). The user enters their correct credentials, and a local login security setting is generated for them at the IdP. Subsequently, the IdP creates an artifact that includes the source ID for its website and a reference to the response message (MessageHandle).

The HTTP artifact binding allows for either HTTP redirection or an HTML form POST to deliver the artifact to the SP. The SP's Assertion Consumer Service sends a SAML ArtifactResolve message to the IdP's Artifact Resolution Service endpoint, using the synchronous Simple Object Access Protocol (SOAP) binding. The IdP's Artifact Resolution Service retrieves the original SAML Response message corresponding to the Artifact and returns it to the SP using the synchronous SOAP binding. The SP processes the response message, extracts and processes the embedded assertion, and creates a local login security setting for the user [15].

However, the use of SOAP binding in this SAML SPInitiated SSO process poses a security risk, particularly as it is vulnerable to a MITM attack [16]. The RelayState token utilized in the process may unintentionally leak information about the user's activities at the SP to the IdP if the SP deployment is flawed or if there are existing vulnerabilities [17]. Additionally, the HTTP Artifact binding's lack of digital signature on the assertion further increases the chances of a MITM attack in SAML, rendering it a notable security concern.

3) DoS Attack in OIDC: To explore the potential for a Denial-of-Service (DoS) attack in OpenID Connect (OIDC), a crucial step is to comprehend the discovery process utilized to acquire the OIDC identity provider's configuration information. The OIDC identity provider (e.g., OpenID provider.com) supports metadata discovery, hosting its configuration information at the endpoint. Often, this endpoint is accessible to any client or relying party intending to send a registration request, making it publicly open and possibly lacking in security measures. As part of the process, the OIDC client or relying party sends an HTTP GET request to this metadata endpoint to obtain the OIDC identity provider's configuration details. In response, the OIDC identity provider provides a set of claims containing essential information about its configuration, including various endpoints and public key locations. These details are necessary for the client or relying party to establish further communication with the OIDC identity provider or the OAuth authorization server.

III. SMART CITY SYSTEM MODEL

Building on the foundational insights collected through the comprehensive literature research, this section defines our distinctive contribution to the field of digital identity management within Smart City ecosystems, demonstrating an innovative approach designed to meet the significant security attacks identified. To establish seamless interoperability among government agencies, the foundation should not solely rely on technology but rather begin with the establishment of a comprehensive government interoperability framework, fostering collaboration, and defining clear policies with a focus on trust. A government-wide policy plays a pivotal role in ensuring the coordination of public agencies and facilitating identity, credential, and access management activities, thereby enhancing access to electronic government services not only within the agencies but also in interactions with other government entities, business partners, and the citizens they serve. The adoption of such a policy framework enhances efficiency, promotes data sharing, and strengthens the overall integrity of the government's digital ecosystem, leading to improved public service delivery and greater citizen engagement.

The present research adopts a system analytical method to propose an interoperability model for digital identity systems in Smart Cities (Figure 1). The model is developed after a literature review and an in-depth analysis of the current interoperability landscape among different services within the Canadian Smart City. It is important to note that the proposed model is considered a preliminary phase and will be subject to refinement in subsequent phases based on technological advancements, standardization efforts, protocol developments, legal regulations, and user acceptance of the new digital identity interoperability system.

 ISBN: 978-1-68558-151-0

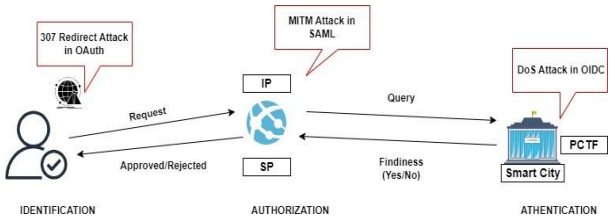

Figure 1. Smart City-Digital Identity Model.

To comprehend the concept of interoperability in this con- text, a digital identity system is envisioned as a collective of multiple Service Providers (SPs) responsible for recording, storing, and processing users' personal information. Each SP operates as its own Identity Provider (IP). Two distinct Service Providers are deemed interoperable if there exists at least one intermediary account on each platform, facilitating the seamless and automatic transfer of the minimum required information in response to legal requests from any account on one SP to any account on the other. In the proposed model, the role of the intermediary account is assumed by the government of the Smart City.

It is important to clarify that this intermediary role does not involve the storage or processing of user information. Instead, the model relies on the existing framework and standards, which facilitate and regulate this intermediary function. The government of the Smart City will be granted the necessary trusted rights to mediate requests between two distinct Service Providers, thereby streamlining the process of user identification and authorization.

IV. USE CASES: SEAMLESS USER AUTHENTICATION IN THE DIGITAL IDENTITY INTEROPERABILITY MODEL FOR SMART CITIES

This use case will help as a road map through the implementation of our model, which address a slew of issues including data exchange, authentication compatibility, privacy management, and regulatory compliance of Canada.

A. Scenario

In the context of the proposed research on digital identity interoperability in Smart City, we consider the use case of a citizen, Alice, who intends to create a public transport account. The process involves the identification and authentication of Alice's identity to ensure secure access to public transport services. The system adopts a government interoperability framework, emphasizing collaboration, clearly defined policies, and trust as the foundation for seamless interoperability across government agencies.

B. Identification

Identification occurs at the initial step when Alice seeks to access a service. She provides her current identifiers to the respective Service Providers she engages with. In this phase, the model has to prevent unwanted access to user credentials, specifically the 307 Redirect Attack in OAuth.

C. Authentication

Following the identification step in which Alice provides her name and surname, the public transport service initiates the authentication process. To verify Alice's identity, the service requests that she present an authenticator. In this case, Alice utilizes her student card as an authenticator to prove her identity. This model addresses authentication compatibility by allowing many types of authenticators, such as student cards, to authenticate identification. This adaptability ensures that the system is able to communicate with existing authentication techniques used by various service providers, allowing for a uniform user experience across all services inside the Smart City. In this phase, the authentication request from Smart City to the university (or vice versa) is securely transmitted using MITM-resistant protocols, and usage of digital signatures.

D. Role of the Smart City

In the proposed model, Smart City plays a crucial role as the intermediary account holder. This role does not entail the storage or processing of user information. Instead, the model leverages the existing framework or standard to facilitate the authentication process. In this way the model enables the secure exchange of information via a trusted intermediary, the Smart City, which verifies identities without directly handling sensitive data. Smart City's infrastructure is intended to resist high rates of requests and protect against DoS attacks. This could include indicating the reliability of the server hosting the OIDC identity provider's configuration information. This approach assures that data communication between service providers and the authenticating institution, in this case public transport service takes place within a regulated and secure environment, reducing the risk of unauthorized access or data breaches.

E. Authentication Request

The public transport service sends an authentication query to Smart City, seeking verification of Alice's student card. Smart City, together with trusted entity PCTF, manages the authentication request and forwards it to the university, where Alice claims to be a student. The trustworthiness of Smart City as part of the digital identity ecosystem ensures prompt and accurate responses from other Service Providers.

F. Authentication Outcome

Upon receiving the query, the university provides a minimal response, confirming Alice's student status "Yes" or denying it as "Not". Smart City then relays the authentication outcome to the public transport service, completing the authentication process.

G. Authorization

The final step of the process involves authorization, where the Service Provider proceeds to grant access to the user's account based on the authentication outcome.

 ISBN: 978-1-68558-151-0

H. Implications

The use case exemplifies the efficacy of the proposed digital identity interoperability model in a Smart City. By leveraging an intermediary account holder and adhering to the current framework or standard, the model streamlines user authentication while minimizing the exposure of personal data. This user- centric approach ensures enhanced privacy, trust, and security in the digital identity ecosystem, offering valuable insights for the advancement of interoperable systems in Smart City and beyond. Additionally, the model's compliance to strictly defined policies and standards indicates its commitment to regulatory compliance, particularly in terms of digital identity verification and data protection legislation. By developing the system to work within an existing framework or standard, the model is better positioned to comply with regulatory requirements, such as privacy and data security.

V. CONCLUSION AND FUTURE WORK

This research addressed the severe security concerns that arise in the pursuit of seamless interoperability within the Identity Access Management (IAM) cycle of digital identity systems, notably in the setting of Smart Cities. The current situation, as demonstrated by the Canadian Federation's decentralized identity management systems, emphasizes the necessity for a single and dependable identification tool. While efforts, such as the Pan-Canadian Trust Framework (PCTF), have been made to create a trustworthy identification ecosystem, the segmented structure of jurisdictional responsibilities has hampered the development of a complete and interoperable solution. As digital identity management evolves, the research emphasizes the need for seamless interoperability, which presents a range of challenges including data exchange, authentication compatibility, privacy management, and regulatory compliance. To address these issues, a proposed system model for Smart Cities is presented, stressing the government's role as an intermediary account holder in allowing secure and transparent identification processes. The approach seeks to achieve a careful balance between resolving security issues and promoting frictionless data interchange, supported by collaboration, standardization, and strong security safeguards. The proposed approach is consistent with the principles of least privilege and segregation of roles, which contribute to a robust and user-friendly IAM cycle. The contributions of this research toward the advancement of secure and user-centric digital ecosystems are noteworthy and facilitate progress in the domain of secure identity management and authentication mechanisms.

As a future work, it is imperative to conduct in-depth investigations into the implementation and practical viability of Zero-Knowledge Proofs (ZKP) for secure identification, ensuring that user data remains confidential while enabling seamless verification across platforms. In addition, as quantum computing advances, comprehensive studies are warranted to explore and adopt quantum-safe encryption techniques, such as lattice-based encryption and hash-based signatures, to fortify digital identity systems against potential quantum threats.

On the other hand, researchers should focus on developing fault-tolerant frameworks that enable automated recovery from transaction failures, enhancing the overall reliability and continuity of the system. Additionally, regulatory and governance bodies must actively reassess existing policies to accommodate Decentralized Identity (DID) and Self-Sovereign Identity (SSI) approaches while upholding data protection principles. Cross- border interoperability and the development of standardized protocols require collaborative efforts across jurisdictions to facilitate secure global transactions.

Furthermore, empowering users with comprehensive knowledge of digital identity concepts and privacy rights through educational initiatives will foster trust and confidence in the system. Finally, exploring novel use cases for digital identity interoperability in various sectors, including finance, healthcare, commerce, education, and travel, will uncover innovative solutions and further reinforce the system's adaptability to diverse scenarios. This future work will significantly contribute to the advancement of digital identity systems in Smart City, fostering a secure, seamless, and user-centric digital ecosystem.

ACKNOWLEDGEMENT

The work reported in this paper has been started as part of an internship offer by the Université de Bretagne-Sud in France as part of the CYBERUS Erasmus Mundus Joint Master program from EU, and by the Université de Sherbrooke in Canada.

REFERENCES

[1] DIACC/CCIAN, "Digital ID for Canadians," https://diacc.ca/, 2024.

[2] M. Lips and J. A. Taylor, "Personal identification and identity management in new modes of e-government," in Economic and Social Research Council, Great Britain, 2007.

[3] A. K. Sharma, S. Sharma, and M. Dave, "Identity and access management- a comprehensive study," in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 1482-1485.

[4] S. Boonkrong, "Authentication and access control: practical cryptography methods and tools," Berkeley, CA, USA: Apress, pp. 45-70, 2021.

[5] J. Bonneau et al., "The quest to replace passwords: A framework for comperative evaluation of web authentication schemes," in IEEEE Symposium on Security and Privacy, 2012.

[6] I. Georgiou et al., "Blockchain for Smart cities: a systematic literature review in Information Systems," in 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, 2020.

[7] Official Publications of the European Communities, "European Interoperability Framework for Pan-European

 ISBN: 978-1-68558-151-0

eGovernment Services," 2004. [Online]. Available: https://op.europa.eu/en/publicationdetail//publication/a4778634-27fa-43b4-9912-f753c4fdfc3f. [Accessed: Mar. 22, 2024].

[8] "e-Government Interoperability: Overview," Report, United Nations Development Programme (UNDP), 2007.

[9] "Canada-EU Joint Workshop Series for Enabling Interoperability and Mutual Support for Digital Credentials," 2021. [Online]. Available: https://digital-trategy.ec.europa.eu/en/library/canada-eu-joint-workshop-series-enabling-interoperability-and-mutual-support-digital-credentials. [Accessed: Mar. 22, 2021].

[10] E. Damiani et al., "Managing multiple and dependable identities," in IEEE Internet Computing, , vol. 7, no. 6, pp. 29-37, 2003.

[11] F. Paci, R. Ferrini, A. Musci, K. Steuer, and E. Bertino, "An interoperable approach to multifactor identity verification," Computer, vol. 42, no. 5, pp. 50-57, 2009.

[12] D. Fett et al., "A comprehensive formal security analysis of OAuth 2.0," in Computer and Communications Security ACM, pp. 1204-1215, 2016.

[13] T. Lodderstedt et al., "OAuth 2.0 threat model and security considerations", Technical report, IETF, 2013.

[14] J. Somorovsky et al., "On breaking SAML: Be whoever you want to be", in 21st USENIX Security Symposium (USENIX Security 12), pp. 397-412, 2012.

[15] A. Armando et al., "An authentication flaw in browser-based single sign-on protocols: Impact and remediations", Computers & Security, vol. 33, pp. 41-58, 2013.

[16] T. Grob, "Security analysis of the SAML single sign-on browser/artifact profile", in 19th Annual Computer Security Applications Conference, pp. 298-307, 2003.

[17] R. Vaughun et al., "Information assurance measures and metrics-state of practice and proposed taxonomy", In the Proceedings of the 36th Annual Hawaii International Conference on System Sciences, IEEE, 2003.

 ISBN: 978-1-68558-151-0

Intelligent Bus Shelter as an Example of the Novel Smart City Technology Integration

Tomasz Wejrzanowski
APPLINK, Trakt Lubelski 137, 04790 Warsaw, Poland
Warsaw University of Technology, Faculty of Materials Science and Engineering, Woloska 141, 02507 Warsaw, Poland
e-mail: tomasz.wejrzanowski@pw.edu.pl

Lukasz Pulka
APPLINK,
Trakt Lubelski 137, 04790 Warsaw, Poland
e-mail: l.pulka@applink.pl

Konrad Owieczko
APPLINK,
Trakt Lubelski 137, 04790 Warsaw, Poland
e-mail: k.owieczko@applink.pl

Piotr Wroblewski
APPLINK,
Trakt Lubelski 137, 04790 Warsaw, Poland
e-mail: p.wroblewski@applink.pl

***Abstract*— In this comprehensive study, an in-depth overview of a multi-stage development project is presented, focusing on the creation of a Demonstrative Version of an Interactive Multimedia Bus Shelter as a component of a novel concept in Smart City infrastructure. The project aimed to address various interesting challenges inherent in developing intelligent bus shelters, encompassing aspects like cost constraints, susceptibility to vandalism, power supply stability, and seamless retrofitting into existing infrastructure. Emphasizing a holistic approach, the designed bus shelter showcased high interactivity, low energy demand through environmentally friendly solutions, and superior functionality. The integrated modules encompassed an intelligent LED (Light Emitting Diode) matrix, LTE (Long Term Evolution) gateway, portable device charger, image acquisition camera, environmental sensor eco-monitor, photovoltaic array, among others. Notably, all these elements were orchestrated through artificial intelligence algorithms, highlighting the system's advanced technological foundation. The investigation results provide a roadmap for the implementation of individual solutions, including an efficient power supply system, a secured and high-performance internal and external communication infrastructure, and an AI (Artificial Intelligence)-based human interactive system. The integration of above elements is likely to represent a solution in creating the intelligent bus shelters of the future - shelters that will be technologically advanced, but also energy efficient, secure, and responsive to the needs of both passengers and the broader Smart City ecosystem.**

Keywords- bus shelter; smart city infrastructure; artificial intelligence.

I. INTRODUCTION

Intelligent bus shelters stand at the forefront of modern urban development, embodying a transformative fusion of technology and public infrastructure. In the evolving landscape of Smart Cities, these shelters play a pivotal role in redefining public transit experiences while showcasing the seamless integration of technology into the very fabric of urban living [1]. Serving as connectivity hubs, these shelters not only enhance accessibility through amenities like Wi-Fi and USB charging, but also seek to meet the digital needs of urban populations in an era characterized by connectivity and convenience [2]. Moreover, their eco-friendly features contribute to sustainability goals, aligning with efforts to create environmentally responsible urban ecosystems [3][4].

This short paper is structured as follows. In Section II, we present our methodology. Section III presents the results and discussion, and we conclude in Section IV with potential applications.

II. METHODOLOGY

This comprehensive study focuses on the multi-stage development of a Demonstrative Version of an Interactive Multimedia Bus Shelter—an integral component of a novel Smart City infrastructure concept. The project addresses various challenges associated with the development of intelligent bus shelters, including cost constraints, susceptibility to vandalism, power supply stability, and seamless retrofitting into existing urban infrastructure.

Emphasizing a holistic approach, the designed bus shelter showcased high interactivity, low energy demand through environmentally friendly solutions, and superior functionality. The integrated modules, driven by artificial intelligence algorithms, included an intelligent LED matrix, LTE gateway, portable device charger, image acquisition camera, environmental sensor eco-monitor, and a photovoltaic array. This integration not only highlights the technological prowess of the system, but also underscores its potential to contribute significantly to the efficiency, connectivity, and forward-thinking nature of Smart Cities.

This study delves into the rigorous testing of the complementary systems, offering valuable insights and guidance for technological solutions. The investigation results provide a roadmap for the implementation of individual solutions, including an efficient and island power supply system [5], a secured and high-performance internal and external communication infrastructure [6], and an AI-

 ISBN: 978-1-68558-151-0

based human interactive system [7]. The integration of these elements represents a significant stride in creating intelligent bus shelters that are not only technologically advanced but also efficient, secure, and responsive to the needs of both passengers and the broader Smart City ecosystem.

III. Results and Discussion

Within the studies discussed in Section II, the construction and smart systems of the Intelligent Bus Shelter was developed and integrated (see Figure 1).

Figure 1. Bus shelter developed within the project.

The entire system considered the following elements and functionalities:

- Internet access point,
- Charging point for mobile devices and personal urban transportation means (e.g., scooters),
- Timetable information, taking into account the estimated current travel time, depending on traffic intensity and unforeseen events, including transfers, with a search function for the fastest connections,
- Line number information for approaching public transport vehicles,
- Information on the current load of approaching public transport vehicles, especially during peak hours,
- Stop request signal and taxi service call feature,
- Assistant for people with disabilities, providing additional information and warnings, as well as conveying the need for assistance during boarding a vehicle.
- Tourist guide, facilitating access to places of historical and architectural significance in the city,
- Ticket vending machine offering electronic tickets for travel,
- Weather station with air quality monitoring and warnings about approaching atmospheric phenomena,
- Monitoring station controlling urban lighting in a specified area, also serving as part of the notification system for medical and law enforcement services,
- Other reporting and information services, with the possibility of future implementation.

In addition, the roof surface of the shelter was used to install photovoltaic panels, providing additional power to electronic systems, thereby reducing the burden on the power grid and contributing to environmental protection.

All the systems were tested for their efficiency and durability in the environmental conditions to prove their applicability for the outdoor operation.

IV. Potential Applications

Due to the diverse and unique functionality, a varied user group is anticipated, extending beyond the commonly understood group of passengers. These groups can be preliminarily identified as:

- Passengers, with special consideration for amenities aimed at individuals with a certain degree of disability,
- Operators of public transportation vehicle networks, including the drivers of these vehicles,
- Meteorological and environmental services (remote weather station, air solution monitoring),
- Rescue and medical services (Automated External Defibrillator - AED, First Aid Kit),
- Traffic control and transportation safety management centers,
- Municipal services - audience measuring capabilities using smart cameras combined with Artificial Intelligence used to strictly define types of potential end users (gender, age, focus time etc.).

Acknowledgment

This work was financially supported by the European Regional Development Fund (ERDF) in the frame of the Polish project “Development of innovative solutions supporting the construction of a smart city – Smart City” No. RPMA.01.02.00-14-d770/20-00.

References

[1] R. P. Dameri and A. Cocchia “Smart city and digital technology: Assessing the role of the firm”. *Technological Forecasting and Social Change*, 142, pp. 70-80, 2019.

[2] T. Nam and T. A. Pardo “Conceptualizing smart city with dimensions of technology, people, and institutions”. Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, pp. 282-291, 2011.

[3] A. Caragliu, C. Del Bo, and P. Nijkamp “Smart cities in Europe”. Journal of Urban Technology, 18(2), pp. 65-82, 2011.

[4] R. Giffinger, C. Fertner, H. Kramar, R. Kalasek, N. Pichler-Milanović, and E. Meijers “Smart cities: Ranking of European medium-sized cities”. Centre of Regional Science (SRF), Vienna UT, 2007.

[5] B. Li, S. Ye, and Y. Feng “Intelligent transportation system based on microgrid for smart city”, Journal of Ambient Intelligence and Humanized Computing, 9(5), pp. 1691-1703, 2018.

[6] Y. Yuan, Y. Geng, and X. Liang “Towards a low carbon and smart transportation in China: A case study of Beijing”, Sustainable Cities and Society, 45, pp. 712-719, 2019.

[7] V. Albino, U. Berardi, and R. M. Dangelico “Smart cities: Definitions, dimensions, performance, and initiatives”, Journal of Urban Technology, 22(1), pp. 3-21, 2015.

 ISBN: 978-1-68558-151-0

Introducing Advanced Comparative Life Cycle Assessment for Evaluating Environmental Conditions and Carbon Opportunity Costs of Energy Production Facilities

Sunghwan Kim
A/E Civil and Environmental Engineering
Stanford University
Stanford, USA
email: sunghwan@stanford.edu

Juyeong Maeng
Excution Design Team
HYUNDAI E&C
Seoul, Korea
email: 2401081@hdec.co.kr

Taehyung Kwon*
A/E Civil and Environmental Engineering
Stanford University
Stanford, USA
email: kwon1579@stanford.edu

***Abstract*—This study introduces an Advanced Comparative Life Cycle Assessment (LCA) model that refines the accuracy of environmental impact evaluations for renewable energy by integrating external factors like sea depth, solar irradiance, and wind speed. Traditional LCA approaches, which often overlook these critical variables, result in imprecise carbon footprint estimations. Developed with Python and incorporating libraries such as SciPy, Windrose, and pvlib, this model provides a nuanced analysis tailored to specific environmental conditions, particularly focusing on Korea. It aims to correct the shortcomings of existing LCA methods by factoring in regional variability, thereby offering more accurate assessments of carbon emissions and environmental impacts of renewable energy projects. This research facilitates informed decision-making in the renewable energy sector by improving the understanding of carbon footprints and supporting sustainable development policies. The study underscores the importance of considering local environmental conditions in the deployment of renewable energy technologies to achieve more sustainable and informed energy solutions.**

***Index Terms*—Life cycle assessment; Carbon opportunity cost; Renewable Energy; Environmental impact; Python-based modeling.**

I. Introduction

During the 29th Conference of Partics (COP) in Dubai in December 2023, the newly adopted "UAE Consensus" emphasized the urgency of transitioning from fossil fuels as an energy source by 2030 [1]. The consensus also included the commitments to triple the current global renewable energy supply, double the efficiency of energy use, and expedite the advancement of low-carbon technologies, with a particular focus on Carbon Capture, Utilization, and Storage (CCUS). Commencing in late 2018, there has been a subtle global surge in the development of new forms of energy, including Energy Storage Systems (ESS) and offshore wind farms, from various nations including Korea, European Unions, Austria, and the United States [2]. This trend has signaled a paradigm shift towards a renewable era, avoiding fossil fuel dependence; further, innovative transitions towards new platforms and technologies dedicated to power transactions are surely expected - getting closer to the ultimate goal of a carbon net-zero world by 2050.

The rest of the paper is structured as follows. In Section II, we examine the need for including external environmental factors in Life Cycle Assessments (LCA) of power generation. Section III details our methodology, describing the development of an Advanced Comparative LCA model and a Python-based environmental impact analysis model. Section IV outlines the expected outcomes, emphasizing the practical applications for stakeholders and policymakers in renewable energy. We conclude in Section V with a summary of our findings and their implications for sustainable energy practices.

II. Significance

Drawing from current studies [3] [4], the assessment of energy production's efficiency and carbon emissions predominantly focuses on the power generation process of energy sources via the Life Cycle Assessment (LCA). Yet, such studies, many times, overlook crucial external environmental factors such as specific production circumstances, airflow, and irradiation. Moreover, in Peer-to-Peer (P2P) power trading scenarios, decisions are typically based solely on carbon emissions associated with the method of power generation [5]. As such, in the context of LCA, there exists a considerable potential for erroneous decision-making. For instance, in solar power generation, there has been a shortage of research to gather data on irradiation and to assess the environmental carbon opportunity cost - defined as the potential for CO2 emissions from the construction and operational processes of energy production facilities - in relation to power production alongside its carbon emission [6] [7]. Moreover, the ample number of studies oftentimes generalize the carbon emission of wind power to be 5 – 9g of CO2/kWh; yet, no differentiations were given either onshore or offshore [8].

On the other hand, other studies on offshore wind power suggest a carbon emission rate of approximately 6 g of CO2/kWh [8]. However, even such studies seldom consider variables such as water depth and wind speed within their LCA. In particular, under the nature of offshore wind power generation, installation depths significantly influence construction costs and carbon emissions [9]. Similarly, for solar power installations, the variability in radiation leads to uncertainty on the unit price and power production per unit of carbon emission. The installation of renewable power plants in locations that do not account for external environmental factors necessitates the evaluation of potential carbon emissions from replacement and repair processes [10]. However, these considerations are currently overlooked in existing LCA methodologies. This omission of external environmental factors could lead to

 ISBN: 978-1-68558-151-0

substantial inaccuracies in the quantification of such actual carbon emissions. For a more precise assessment, this study consider not only the resources expanded on energy facilities but also the external environmental factors influencing their efficiency and impact.

III. METHOD

A. Development of the Advanced Comparative Life Cycle Assessment Model

Numerous previous studies and tools have been only developed to simply quantify the electricity yield of solar power installations, using local solar irradiance data. In this research, we are in the process of developing the Advanced Comparative Life Cycle Assessment model, which is an enhanced approach to the existing life cycle assessment, improving traditional methodologies by incorporating distinct environmental factors - sea depth, solar irradiance, and wind speed - to suit the various ecological locations in the context of Korea, as a prototype. The traditional methodologies approaches often overlook regional environmental variations - in terms of varying amounts of solar irradiance, and wind speed with varying altitude - potentially leading to inaccurate emission assessment in proportional relation to their different temporal efficiency of generation. By factoring in such locational variability and specificity, the proposed assessment provides a more precise quantification of environmental impacts and carbon emissions per unit of the electricity yield under diverse conditions, automating the carbon opportunity cost.

B. Python-Based LCA Model for Environmental Impact Analysis

Building on this foundation, our work has led to the development of a Python-based Life Cycle Assessment model. Utilizing Python as a scripting language, the model is intricately designed to provide a detailed analysis of the environmental impacts associated with renewable energy projects, with a special focus on construction costs and carbon emissions. The model integrates the SciPy library for its extensive applications in scientific and technical computing for sophisticated algorithms for numerical analysis. Additionally, by incorporating specialized libraries such as Windrose and pvlib, the model is uniquely equipped to model and study wind and solar power, respectively. As a prototype, the model stores backend data such as sea depth, average sunlight, and wind speed specific to Korea, intending to calculate the expected carbon emissions and installation costs for new renewable energy facilities based on their location. From the user interface, users can select various options like the power generation method and scale, materials for the power plant and its foundation, and the total amount of materials used. This allows for a comparison of carbon emissions and power efficiency with the backend Python calculation results, thereby providing a multifaceted approach to analyzing the environmental impacts of renewable energy projects.

This model, ultimately, aims to enhance the societal understanding of carbon footprints by processing inputs that include the specific characteristics and locality of renewable energy facilities, leveraging Korean public datasets to dynamically update environmental factors such as wind speed and solar irradiance based on location, and incorporating contemporary raw material import costs. By evaluating these parameters over a 20-year lifespan through complex unit conversions and theoretical calculations, the model delivers a comprehensive LCA.

IV. EXPECTED OUTCOME

The purpose of the study extends beyond its technical aspects. The assessment model is aimed to provide useful environmental impact analysis by providing such valuable information accessible to a broader audience. Through this, the study aims to allow stakeholders to make informed decisions about renewable energy, and its resources in specific locales, thus, offering more accurate, localized, and environmentally conscious perspectives. Specifically, the function of the model is being proposed to be beneficial to the business sectors in renewable energy and to general users, especially in the context of P2P power transactions. It is designed for companies to employ this model to improve efficiency and carbon emissions of their energy production processes, while general users gain the ability to conveniently select electricity generators, based on their simple carbon emission values. Ultimately, this advancement in such perspectives must allow further sustainable development and aid informed policymaking, underling the benefits of this approach.

REFERENCES

[1] "The Global Stocktake at COP28," Nature Climate Change, vol. 13, no. 11. Springer Science and Business Media LLC, pp. 1146–1147, Oct. 13, 2023.

[2] F. Mohamad, J. Teh, C.-M. Lai, and L.-R. Chen, "Development of Energy Storage Systems for Power Network Reliability: A Review," Energies, vol. 11, no. 9. MDPI AG, p. 2278, Aug. 30, 2018.

[3] S. Verma, A. R. Paul, and N. Haque, "Selected Environmental Impact Indicators Assessment of Wind Energy in India Using a Life Cycle Assessment," Energies, vol. 15, no. 11. MDPI AG, p. 3944, May 26, 2022.

[4] J. Chipindula, V. Botlaguduru, H. Du, R. Kommalapati, and Z. Huque, "Life Cycle Environmental Impact of Onshore and Offshore Wind Farms in Texas," Sustainability, vol. 10, no. 6. MDPI AG, p. 2022, Jun. 14, 2018.

[5] F. Asdrubali, G. Baldinelli, F. D'Alessandro, and F. Scrucca, "Life cycle assessment of electricity production from renewable energies: Review and results harmonization," Renewable and Sustainable Energy Reviews, vol. 42. Elsevier BV, pp. 1113–1122, Feb. 2015.

[6] R. Turconi, A. Boldrin, and T. Astrup, "Life cycle assessment (LCA) of electricity generation technologies: Overview, comparability and limitations," Renewable and Sustainable Energy Reviews, vol. 28. Elsevier BV, pp. 555–565, Dec. 2013.

[7] D. Ravikumar, G. Keoleian, and S. Miller, "The environmental opportunity cost of using renewable energy for carbon capture and utilization for methanol production," Applied Energy, vol. 279. Elsevier BV, p. 115770, Dec. 2020.

[8] Y. Wang and T. Sun, "Life cycle assessment of CO2 emissions from wind power plants: Methodology and case studies," Renewable Energy, vol. 43. Elsevier BV, pp. 30–36, Jul. 2012.

[9] H. Chen, H. Yu, X. Yang, Y. Lin, S. Lou, and S. Peng, "Joint Planning of Offshore Wind Power Storage and Transmission Considering Carbon Emission Reduction Benefits," Energies, vol. 15, no. 20. MDPI AG, p. 7599, Oct. 14, 2022.

[10] A. Garcia-Teruel, G. Rinaldi, P. R. Thies, L. Johanning, and H. Jeffrey, "Life cycle assessment of floating offshore wind farms: An evaluation of operation and maintenance," Applied Energy, vol. 307. Elsevier BV, p. 118067, Feb. 2022.

[11] S. Ku, S. Kim, M. You, and M. D. Whitaker, "Building the Groundwork for a Natural Search, to Make Accurate and Trustworthy Filtered Searches: The Case of a New Educational Platform with a Global Heat Map to Geolocate Innovations in Renewable Energy," Intelligent Human Computer Interaction. Springer Nature Switzerland, pp. 239–250, 2023.

 ISBN: 978-1-68558-151-0