A CYBER SECURITY ONTOLOGY FOR SMART CITY

Tehreem Qamar, Narmeen Zakaria Bawany

Center for Computing Research
Department of Computer Science and Software Engineering
Jinnah University for Women
e-mails: tehreem.qamar@juw.edu.pk, nsb@juw.edu.pk
Pakistan

Abstract: Smart city is an intelligent and interconnected city that aims to enhance the quality of living of its people by using information and communication technology (ICT). However, the intrinsic inter-connectivity makes it highly vulnerable to security attacks. Therefore, it is essential to build a robust architecture that not only offers smart city services but also satisfies its security issues. This paper presents an integrated layered architecture for smart city security named ICADS. Moreover, two semantic models of ICADS are proposed as ontologies, namely OntoICADS and Secure-OntoICADS, to deal with the dynamicity and security of smart city. Secure-OntoICADS provides formal description to four major elements of security i.e. vulnerability, attack, security requirement, and security mechanism. Additionally, to validate their adaptability, ontologies have been mapped to different smart city applications.

Key words: Smart city, cyber security, ontology.

1. INTRODUCTION

The **smart city** is described by its capacity to incorporate people, technology innovation and data to develop a resilient, strong and sustainable infrastructure that gives topnotch administrations to its inhabitants. Transforming an urban city into a smart city requires community oriented endeavors between government, industry, experts, citizens and researchers [1].

Smart city is not only about deploying smart platforms and carry out related services efficiently but it is a huge concept comprising several electronic objects which interact and communicate through wired and wireless networks [2]. Being a massive interconnected framework, smart city brings gigantic challenges. Collaboration among stakeholders, availability and scalability of infrastructure, costs and funding, continually changing people's needs, privacy, security, user-friendly interfaces and interoperability are examples of problems that smart cities face most [2,3,4]. In this paper, we focus on the security of smart cities and present an

integrated framework since information security is one of the critical challenges that can cause catastrophic damage, if not addressed promptly. [2,5].

Smart city generates variety of data from different applications [6] and to manage this heterogeneity, ontology has been used as a promising tool [6,7,9]. Therefore, this paper proposes an ontological framework for security of smart city. The motivation behind employing ontology is to better recognize, define and reuse the represented knowledge base.

The novel contribution of the paper is that it presents an ontology-based representation of smart city, Secure-OntoICADS, which embeds cybersecurity at each level. The Secure-OntoICADS includes all aspects of smart city along-with security and it also standardizes the definitions of data through a common and controlled vocabulary. Moreover, it makes the semantic relationships among the smart city applications and cyber security controls explicit and clear to all stakeholders. Such an approach not only makes the data integration process among various smart city applications unambiguous but also facilitates incorporating security controls at each level. Following are the main contribution of the paper:

- A layered architecture for smart city security has been proposed
- Data organization with semantic knowledge which include security aspects of smart city is presented
- An ontological framework for smart city application, communication and data management is presented with different use cases

The rest of the paper adheres to the structure as follows. Section II presents related work; Section III explained the proposed framework in detail. Section IV describes the use cases for the proposed ontology and Section V concludes the paper with future considerations.

2. RELATED WORK

Ontologies have been widely used to represent the conceptual frameworks. However, cyber security of smart city is pertained by limited number of studies. Though, smart city and network security separately have been part of numerous research studies. This section comprise of the architectures and ontological frameworks of smart city, available ontologies for cyber security and the ontologies presented for cyber security of smart city.

Smart city is a strategy of mitigating the problems generated as a result of urban population growth and their needs. In this regard, key dimensions have been highlighted, depicted in Fig. 1, by the research community on which numerous architectures have been proposed. Fig. 1 shows various domains for which smart city applications are being developed. These domains have varying security requirements. Federico et al. [10] proposed an Internet of Things (IoT) based Service Oriented Architecture for smart city. Network-connected objects will publish their services, which will allow them to be accessed from mobile clients, making communication with human to machine and vice versa more flexible. Bawany et al.

[3] proposed a layered architecture of smart city for providing smart governance. The architecture provides a hierarchical model of data storage and exemplifies how different stakeholders of the city contribute in offering smart city services. Paola et al. [10] presented a fog computing based multi-tiered architecture. It provides smart computation between connecting devices to compute, route and communicate with one another in order to decrease the latency and improve energy provisioning. Along with the aforementioned conceptual models, numerous ontological frameworks have also been proposed. Tarek et al. [11] proposed an ontological framework for existing smart city applications. Authors in [12] provide a smart city ontology which can map smart city services applications.

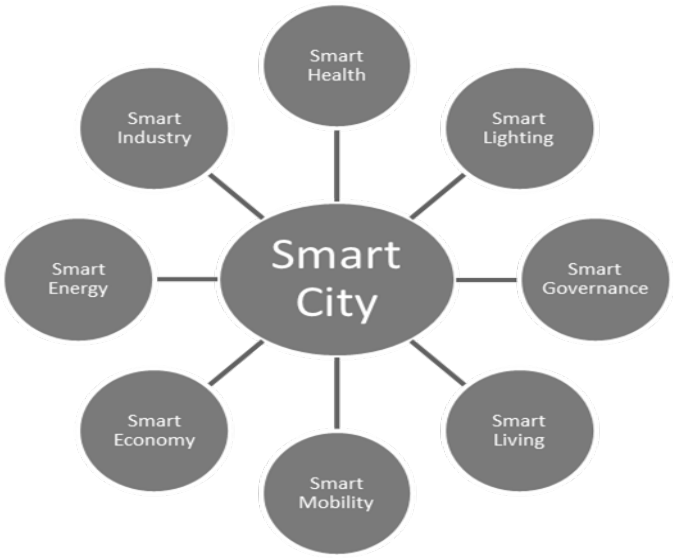

Fig. 1. Smart City Key Dimensions

The scientific community enormously contributed in defining ontologies for cyber security domain. Almut et al. [13] presented an exhaustive ontology on Information security in OWL. The authors claimed that the proposed ontology can be used as a dictionary or a general vocabulary for information security domain. The ontology models vulnerabilities and threats on assets with countermeasures. The authors also presented a set of inferences that can be done on it and demonstrate querying their ontology via SPARQL. Razzaq et al. [14] presented an attack ontology which they believe can improve the detection of attacks on web applications. Pinkston et al. [15] produced a target-centric ontology for intrusion detection system (IDS). They analyzed 4000 classes of computer intrusions and their corresponding strategies and defined relationships which are observable and measurable by the target of an attack. Anoop et al. [16] proposed an ontological model for enterprise level security. They modeled each security threat and its countermeasure with cost, effort and loss metric and claimed that analysis of risk via

ontology enables the enterprise management in defining effective mitigation mechanism. Syed et al. [17] presented a unified cyber security ontology which they believe can serve as DBpedia [18] for cyber security domain. It is an extension of the IDS ontology of Pinkston et al. [15] and integrates heterogeneous schemas from various cyber security systems.

The application of ontology in security of smart city is an emerging area and only few related studies have been found in recent years. Tao et al. [19] presented an ontology-based security management model to enable effective and seamless interactions on heterogeneous devices in IoT-based smart homes. Petrenko et al. [20] develops a cyber-security ontology for smart grid. The ontology provides resistance as per the requirement of energy security and rapidly reestablishing capacities of smart grid after accidents. Most of the existing ontology based studies in terms of cyber security of smart city are limited to one application scenario which affects their application value. To fill this gap, this work proposes cyber security ontology for smart city that can be adapted for any given scenario of smart city.

3. ICADS – THE PROPOSED ARCHITECTURE

The **Smart city** is considered as an instrumented, interconnected and intelligent system [21]. The instruments refer to usage of IoT devices; interconnected means its infrastructure and communication capability and intelligent denotes its artificially intelligent data processing ability. Section II presents numerous architectures that have been proposed to improve real-world deployment of smart cities. However, defining universal smart city architecture is still a focus of research community [8, 22, 23]. After thorough analysis of multiple existing architectures and the definition of smart city mentioned before, we deduce the smart city architecture. Fig. 2 depicts a proposed architecture- ICADS, that comprises of widely adopted four layer smart city architecture with security layer running through all layers.

The architecture consists of infrastructure, communication, application, data and security layers. Infrastructure layer contains sensors, actuators and all related IoT devices. Communication layer comprises of wired and wireless network connectivity mechanisms. Application layer encompasses smart city services for all stakeholders of smart city while Data layer holds all the data generated as a result of any communication within the smart city. To ensure security, a layer surrounds the prior layers incorporating security requirements, vulnerabilities and protection mechanisms for each layer.

ICADS is a simple layered architecture that is based on a four layer smart city model given by many researchers. However, the security aspect of each layer is a novel contribution of ICADS. The focus of this research is to present an ontology that can be used to develop secure smart city applications. The aim of this research is to encourage development of smart city applications that takes into account cyber security requirements at each level, such highly secure and reliable smart city solutions can be deployed.

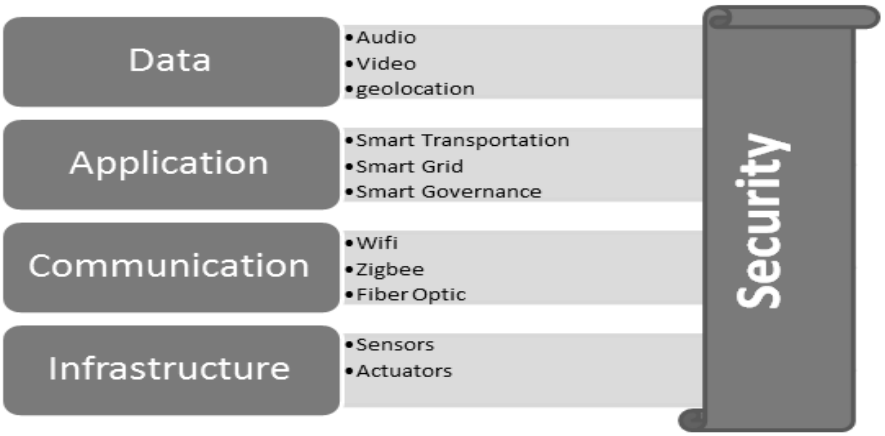

Fig. 2. ICADS – Proposed Smart City Architecture

Smart city is a huge infrastructure comprising of diverse subsystems generating different types of data. Hence, data heterogeneity is one of the prominent characteristics of smart city. Therefore to make the data consistent and easy to share, the ontology for ICADS is proposed in the successive section.

3.1. OntoICADS – Proposed Ontology

OntoICADS defines a centralized data model for ICADS. It represents the classes and relationships between its layers. The notion is depicted in Figure 3. OntoICADS consists of four major classes namely; Infrastructure, Communication Channel, Data and Application. These classes are linked via object properties and because each successive layer can communicate with the previous layer, inverse object properties are also defined respectively.

Infrastructure: comprises of several sub classes which include all IoT devices. The related data properties are defined accordingly.

Communication Channel: This class deals with the communication layer of ICADS. It is divided into two subclasses namely WiredCommunication and WirelessCommunication. These two subclasses are further divided into different classes such as satellite, access point, router, and switch.

Data: This class deals with the storage of data generated within smart city

Applications: This class includes all smart city services application that is available to its inhabitants such as smart parking, smart garbage control, smart street light management, smart complaint management and smart grid.

The aforementioned classes are linked via object properties which provide interoperability among them. The objects of Infrastructure classes can use any communication channel to transmit their data. Hence infrastructure class is connected with communication channel class via **generateData** and **communicateData** object properties. All applications are capable of manipulating

data therefore **manipulates** and **isManipulatedBy** object properties links these two classes. Moreover, data will be transmitted via some communication channel therefore these two classes get linked by **transmits** and **receives** properties. Apart from object properties, appropriate data properties are defined for each class.

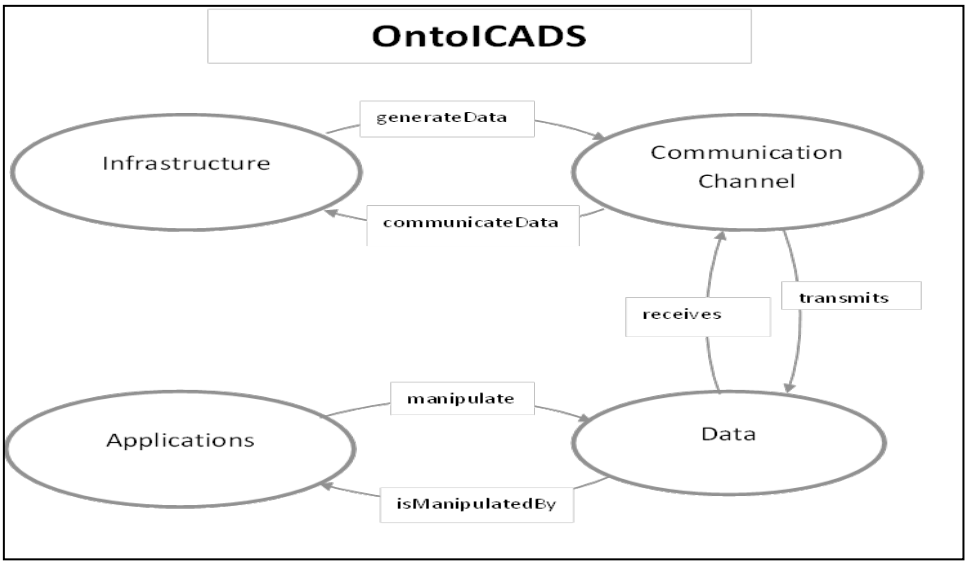

Fig.3. OntoICADS: Proposed Ontology for ICADS

3.2. Secure-OntoICADS

Secure-OntoICADS is the extended version of OntoICADS to secure each layer of ICADS. It comprises of five major classes, namely: Vulnerabilities, Attacks, Security mechanisms, security requirements and impact. Figure 4 illustrates the Secure-OntoICADS ontology.

Vulnerabilities: The security flaws, defects, or bugs in the software and hardware that can be exploited by attackers are referred to as vulnerabilities. In Secure-OntoICADS, the vulnerabilities respective to each layer of the smart city are the subclasses of Vulnerabilities class. Connection of OntoICADS with this class makes each layer aware of the possibility of any attack.

Attacks: This class is divided into two classes i.e. ActiveAttack and PassiveAttack. These two subclasses are further divided into types of attacks.

Impacts: This class measures the severity of attacks and is subdivided into three classes i.e. Catastrophic, Moderate, Low

Security Mechanisms: This class holds the security mechanisms that can apply to each layer. It is directly connected to OntoICADS via object properties and hence provides security to each layer of ICADS.

Security Requirements: This class comprises of security requirements that must be satisfied by security mechanisms.

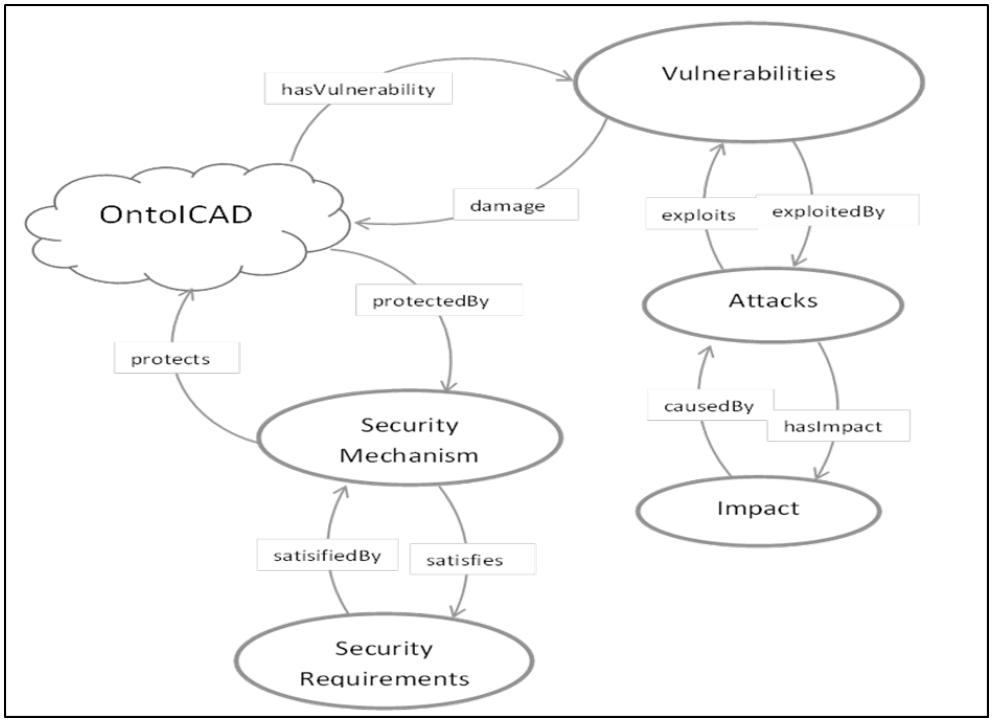

Fig. 1. Secure-OntoICAD

Table 1. Security attributes for Secure-OntoICADS

	Infrastructure Layer	**Communication Layer**	**Data Layer**	**Application Layer**
Attacks	-Theft -Device Hijacking	-Eavesdropping -Man in the middle -Interception -Jamming -Protocol Violation	-Data and Identification theft -Unauthorized access	-Application flooding -Application lockout -Malware injection -Buffer overflow -Device threshold manipulation
Vulnerabilities	-Physical security -The life time of power system	-Greater number of intelligent devices	-Customer Security	-Using internet protocol (IP) and commercial of the shelf hardware and software
Security Requirements	-Confidentiality -Integrity -Availability	-Confidentiality -Integrity -Availability -Authenticity	-Confidentiality -Integrity -Availability -Privacy	-Confidentiality -Integrity -Availability

4. EXAMPLES

This **section** presents the use cases of the proposed ontology. Each use case is first mapped to the OntoICADS and then corroborates the Table 1 to achieve the security measures via Secure-OntoICADS. Table 1 state the security attributes regarding each layer of ICADS.

4.1. Smart Grid

Smart grid is an electric grid which integrates traditional electric power grid with Information and Communication Technologies (ICT) [24]. It entails a centralized electricity network that connects smart devices, suppliers and consumers in order to manage demand, save energy and reduce costs [25].

Figure 5 represents the smart grid in terms of OntoICADS. Smart home appliances, connected to HomeAreaNetwork, use ZigbeeHome as the communication channel while the data transmitted to GridDataCenter uses IPv6 protocol. HomeAreaNetwork and NeighborhoodAreaNetwork uses Infrastructure layer, ZigbeeHome, IPv6 uses communication layer, GridDataCenter is a part of Data layer while the service provider is using application layer.

The security layer of ICADS is attained by mapping Table 1 according to Secure-OntoICADS ontology. Each layer's potential attacks, vulnerabilities and security requirements can be easily logged which will support the mitigation process.

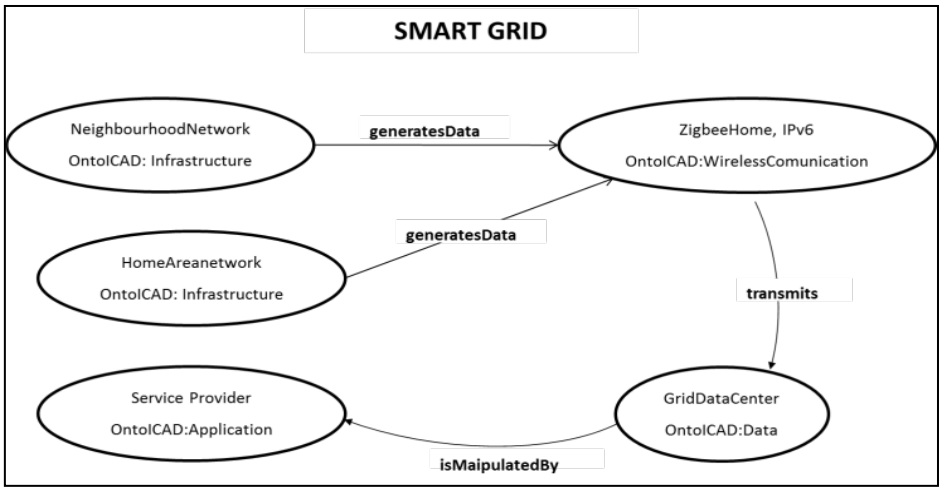

Fig. 2. Smart Grid Scenario for OntoICADS

4.2. Smart Traffic Management

In **Smart Cities**, the key crossing point control is acknowledged by directing the related traffic signals. Traffic signals at a convergence are composed by a traffic light framework under specific guidelines and rules [26]. Figure 6 illustrates the main components of traffic light system in terms of OntoICAD.

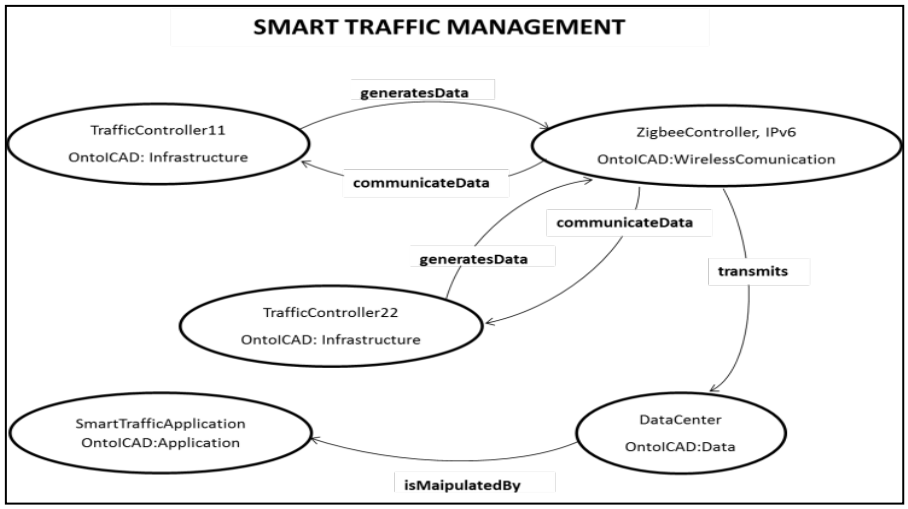

Fig. 6. Smart Traffic Management scenario using OntoICADS

Traffic controllers installed in different areas communicate the road condition via ZigbeeController orIPv6 to the data centre, the data is then manipulated by the smart traffic management application. Similar to the example presented above, the Table 1 attributes are incorporated to each layer to satisfy the security.

4.3. Smart Parking

Smart parking is a way of communicating available parking slots to the drivers searching for a nearby parking place to resolve congestion problem on roads [27]. Figure 7 depicts the system with regard to OntoICADS.

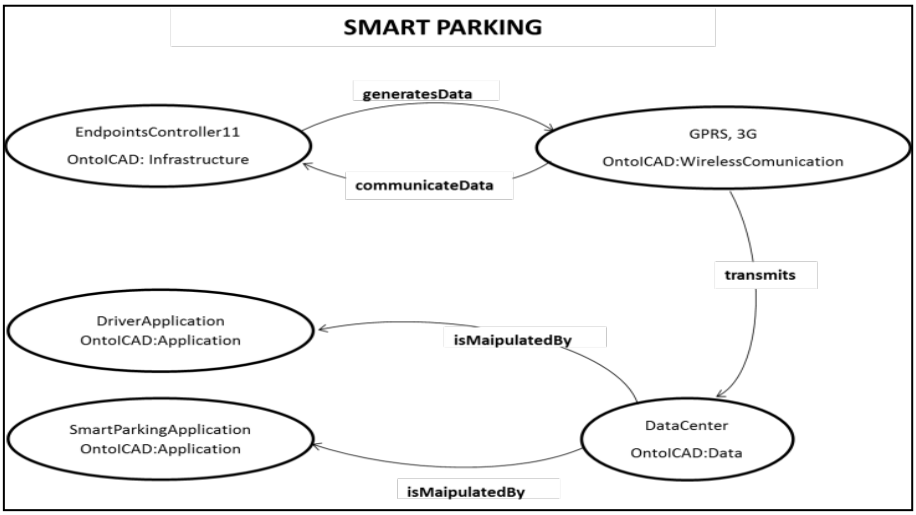

Fig. 7. Smart Parking scenario via OntoICADS

The sensors and actuators installed in parking area are controlled via EndpointController11, instance of Infrastructure class, via GPRS or 3G technology. The data is retained by DataCenter which is manipulated by different applications related to smart parking. All elements are protected according to the security attributes mentioned in Table 1.

Along with aforementioned scenarios, the OntoICADS has the capability to accommodate almost all smart city utilities and related applications.

5. CONCLUSION AND FUTURE WORK

We present an ontological framework for security of smart city Secure-ICADS. The proposed framework is an attempt to provide semantically structured data in terms of security and a shared vocabulary among all smart city applications. Moreover, potential attacks and their associated vulnerabilities are mapped which can detect the probability of a certain attack. It also has the capability to accommodate multiple types of smart city applications. We plan to further extend the ontology by introducing inference rules which would highly help in monitoring the overall network situation of smart city and support in taking effective decisions.

REFERENCES

[1] N. Villanueva-Rosales, R. L. Cheu, A. Gates, N. Rivera, O. Mondragon, S. C. C. Ferregut, C. Carrasco, S. Nazarian, H. Taboada, V. M. Larios, L. Barbosa-Santillan, M. Svitek, O. Pribyl, T. Horak, and D. Prochazkova, "A collaborative, interdisciplinary initiative for a smart cities innovation network," in *2015 IEEE 1st International Smart Cities Conference, ISC2 2015*, 2015.

[2] A. Aldairi and L. Tawalbeh, "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies," in *Procedia Computer Science*, vol. 109, 2017, pp. 1086–1091.

[3] N. Z. Bawany and J. A. Shamsi, "Smart City Architecture : Vision and Challenges," *International Journal of Advanced Computer Science and Applications*vol. 11 (vol.6), 2015, pp. 246–255.

[4] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," *Journal of Advanced Research*, 4 (vol. 5), 2014, pp. 491–497.

[5] N. Z. Bawany and J. A. Shamsi, "SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks," *Journal of Network and Computer Applications*, vol. 145, 2019, p. 2020.

[6] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, "Smart cities of the future," *Eur. Phys. J. Special Topics*, vol. 214, 2012, pp. 481–518.

[7] I. A. T. Hashem, V. Chang, N. B. Anuar, K. Adewole, I. Yaqoob, A. Gani, E. Ahmed, and H. Chiroma, "The role of big data in smart city," *International Journal of Information Management*, 5 (vol. 36), Oct. 2016, pp. 748–758.

[8] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, Jul 2018, pp. 46134–46145.

[9] S. J. Clement, D. W. McKee, and J. Xu, "Service-Oriented Reference Architecture for Smart Cities," in *Proceedings - 11th IEEE International Symposium on Service-Oriented System Engineering, SOSE 2017*, 2017, pp. 81–85.

[10] "A scalable architecture for geo-localized service access in smart cities - IEEE Conference Publication." [Online]. Available: https://ieeexplore.ieee.org/document/6095263. [Accessed: 15-Feb-2020].

[11] T. Abid, H. Zarzour, M. R. Laouar, and M. T. Khadir, "Towards a smart city ontology," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, 2017.

[12] T. Qamar, N. Z. Bawany, S. Javed, and S. Amber, "Smart City Services Ontology (SCSO): Semantic Modeling of Smart City Applications," in *Proceedings - 2019 7th International Conference on Digital Information Processing and Communications, ICDIPC 2019*, 2019, pp. 52–56.

[13] A. Herzog, N. Shahmehri, and C. Duma, "An Ontology of Information Security," *International Journal of Information Security and Privacy (IJISP)*, 4 (vol. 1), 2007, pp. 1–23.

[14] A. Razzaq, Z. Anwar, H. F. Ahmad, K. Latif, and F. Munir, "Ontology for attack detection: An intelligent approach to web application security," *Computers and Security*, vol. 45, Sep. 2014, pp. 124–146.

[15] J. Pinkston, J. Undercoffer, A. Joshi, and T. Finin, "A Target-Centric Ontology for Intrusion Detection." in *Workshop on Ontologies in Distributed Systems, held at The 18th International Joint Conference on Artificial Intelligence, 2003.*

[16] A. Singhal and D. Wijesekera, "Ontologies for modeling enterprise level security metrics," in *ACM International Conference Proceeding Series*, 2010.

[17] L. M. and A. J. Zareen Syed, Ankur Padia, Tim Finin, "UCO-A Unified Cybersecurity Ontology," *Association for the Advancement of Artificial Intelligence*, 2016, pp. 195–202.

[18] C. Bizer, J. Lehmann, G. Kobilarov, S. Auer, C. Becker, R. Cyganiak, and S. Hellmann, "DBpedia - A crystallization point for the Web of Data," *Journal of Web Semantics*, 3 (vol. 7), Sep. 2009, pp. 154–165.

[19] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Generation Computer Systems*, vol. 78, Jan. 2018, pp. 1040–1051.

[20] S. A. Petrenko and K. A. Makoveichuk, "Ontology of Cyber Security of Self-Recovering Smart GRID." in *CEUR Workshop, 2017*, pp. 98-106.

[21] D. Susane, M. Keeling, "A vision of smarter cities How cities can lead the way into a prosperous and sustainable future", *IBM Institute for business*, vol. 8, 2009.

[22] B. N. Silva, M. Khan, and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustainable Cities and Society*, vol. 38. Elsevier Ltd, 01-Apr-2018, pp. 697–713.

[23] Z. Allam and P. Newman, "Redefining the Smart City: Culture, Metabolism and Governance," *Smart Cities*, 1 (vol. 1), Jul. 2018, pp. 4–25.

[24] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart Grid Security: Threats, Vulnerabilities and Solutions," *International Journal of Smart Grid and Clean Energy*, 2012, pp. 1–6.

[25] J. Jackson, "Smart Grids: An Optimised Electric Power System," in *Future Energy: Improved, Sustainable and Clean Options for our Planet*, Elsevier Inc., 2013, pp. 633–651.

[26] Z. Li, D. Jin, C. Hannon, M. Shahidehpour, and J. Wang, "Assessing and mitigating cybersecurity risks of traffic light systems in smart cities," *IET Cyber-Physical Systems: Theory & Applications*, 1 (vol. 1), 2016, pp. 60–69.

[27] M. Alam, D. Moroni, J. Ferreira, G. Pieri, M. Tampucci, M. Gomes, and G. R. Leone, "*Real-Time Smart Parking Systems Integration in Distributed ITS for Smart Cities*," 2018.

Information about the authors:

Tehreem Qamar – Lecturer in Department of Computer Science and Software Engineering, Jinnah University for Women, Karachi, Pakistan. Her research interests include machine learning, semantic web and human computer interaction.

Narmeen Zakaria Bawany – Chairperson of Department of Computer Science and Software Engineering, Jinnah University for Women, Karachi, Pakistan. She has over 15 years of teaching experience at graduate and under graduate level. She has supervised many under graduate projects and had also received funding from ICT R&D for under graduate projects. Her research areas include human computer interaction, machine learning, semantic web, cyber security and software defined networking.

Manuscript received on 30 May 2020