Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

CYBER SECURITY CHALENGES OF PROTECTING SMART CITIES SUSTAINABILITY

Krasimir SHISHMANOV

PhD, Professor,
D. A. Tsenov Academy of Economics, Bulgaria,
ORCID 0000-0001-9874-2149
E-mail: k.shishmanov@uni-svishtov.bg

Iskren TAIROV

PhD, Head Assist. professor,
D. A. Tsenov Academy of Economics, Bulgaria,
ORCID 0000-0002-2971-5451
E-mail: i.tairov@uni-svishtov.bg

Abstract: *Smart cities provide many positive implications that aim at transforming the everyday lives of individuals. This includes enhancing profitability, lowering expenses, and lowering ecological impact, but the smart city concept remains in its infancy. Considering the system mostly relies on electronics, it lets the entryway to hacking attempts and criminals, which might lead to serious harm and potential dangers. A continuing concern is the psychological and formal aspects of smart city protection that have been the result of competing interests, extensive interconnectedness, and cultural and administrative complexities. Due the results of our review, present laws and directions are insufficient to identify the positions and responsibilities of different companies and citizens do not have the same understanding of critical safety requirements. The research carried out assessed smart cities' cyber security initiatives, with a focus on technology demands and legislative architecture. According to the analysis conclusions, the present research argued for an apparatus that comprises technical norms, managerial input, a regulatory mechanism, and conforming verification to ensure security is monitored throughout all phases in smart cities.*

Keywords: *smart cities, security, measures, deep learning.*

UDC: *004.056*

JEL Classification: *L86.*

INTRODUCTION

The concept of a "smart city" denotes the integration of current structures with established communication and information technologies with the objective of developing a seamless system of functional recreational opportunities [1]. A smart city connects physical possessions, technical infrastructure, social infrastructure, and business facilities to strengthen the city's collaborative thinking [2]. Smart cities are enormous, complicated, and technologically dependent, and they face a wide range of technical, financial, electoral, and social challenges. Some of the issues and obstacles that smart cities face are socioeconomic and technological concerns, individual ever-shifting requirements, teamwork across interested parties, easy to implement connecting, and security and stability. Smart cities provide six key components: smart governance, intelligent individuals, smart business, intelligent transportation, environment, and lifestyle [3]. Smart cities meet the needs of organizations, people, and governments by delivering appropriate and effective solutions. Urban support could be expanded in the ecological, tourism, well-being, departure, energy sectors, and home security sectors [4]. Considering the benefits of smart cities for residents, companies, the environment, etc, smart cities are subject to many

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

security concerns, making enabling sustainable growth difficult to accomplish. A dangerous action by an individual or group in a smart city may endanger the entire community [5]. That type of complex metropolis additionally poses a substantial challenge for automated court investigations.

Ensuring privacy in a smart city includes safeguarding data and the architecture against attacks and illicit activity. Suppliers seldom examine the cyber-security of smart city devices and their software. As a result, employing certain vulnerable things can lead to the connection being filled with forged information, the network being taken off, or the equipment malfunctioning as a result of infiltration [6]. Aside from information security, another issue to be worried about is the protection of individual privacy and contacts with authorities [7]. The risk of personal information breaches and a lack of security measures in smart cities might render public acceptance of these advancements difficult. Recognizing cyber security challenges and threats to citizens' privacy is the first step toward overcoming security issues in smart cities and preserving citizens' confidentiality. Individuals cannot expect a smart city to be created, carried out, and grown effectively until the aforementioned problems are addressed and appropriate solutions are offered [8].

LITERATURE REVIEW

Cyber security concerns and dangers to user anonymity in smart cities have been examined by many experts through several perspectives, among which prominent ones are included beneath.

A study highlighted the protection of infrastructure as a successful influence on data and data security in smart cities in a complete evaluation of studies linked to significant safety issues and current remedies in smart cities [9]. There exist numerous hazards and weaknesses associated with urban intelligence's physical-cyber foundation advantages. In the main physical-cyber systems, city infrastructure, involving power and water supply, roadways, structures, and so on, confronts multiple security concerns. Imaging devices, communication networks, management of building platforms, and systems for managing transportation are examples of these parts and technologies.

Another study classified privacy issues as interaction and corporate protection [10]. Eavesdropping, denial of service, fraudulent control and assaults, route incidents, identification, and subsequent usage were all hurdles to achieving privacy. Furthermore, phishing corporate security risks comprised frauds and attempts on data reliability. Other authors offered an exhaustive analysis of a smart city protection potential, highlighting safety issues and providing extensive insight into digitized smart city assessments [11]. According to city organizations, they highlighted security concerns such as smart grids, automated building integrity, aircraft security, smart automobiles, Internet of Things (IoT) sensors, and cloud infrastructure.

Authors like Arabo explored the features and difficulties of smart gadget cyber-security in linked intelligent structures [12]. He researched some of the historical details connected to the growth and need for integrating technology to offer people with various capacities and skills. Furthermore, he demonstrated that, notwithstanding their potential, these innovations are not without risks and obstacles. Lastly, he addressed cyber-security concerns with smart gadgets in linked intelligent structures. Based on the paper, the key issues confronting autonomous structures are breaches of privacy, altering corruption of information, and infection. Thing evaluated the prospects for current global smart cities, as well as the security problems and challenges in any of their major domains [13]. He

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

discussed the use of cyber security to build a smart, secure, and enjoyable city. He outlined security difficulties as well as worries that important sectors of the smart city face, such as banking, medical care, governance, power, and overall safety. Khatoun and Zeadally defined smart city design fundamentals and examined innovative smart city plans [14]. They explored multiple remedies, proposals, and norms connected to these concerns, especially after describing many security concerns and security holes in smart cities. Furthermore, they investigated the fundamental difficulties confronting smart cities through the viewpoints of smart city information security design and the privacy and security issues of various smart city components.

To guarantee cyber security and confidentiality in smart cities, some researchers suggested all three planning and execution assessments for encoding, authorization for use, verification, and firmware upgrades when carrying out fresh initiatives, traditional and safe denial in all urban infrastructure, and developing working strategies and processes for reacting to cyber attacks [15]. Cerrudo and others offered a few of the greatest viable smart city cyber-security strategies [16]. In that study, institutions were given recommendations for selecting and testing smart city-related solutions. The study focused on developing appropriate assessment and validation methodologies for picking such technologies and their associated providers. Other authors conducted a broad examination of existing cyber-security according to six machine-learning categories [17]. Researchers suggested prospective research topics in cyber-security. Another study from 2020 suggested a multi-view composite technique for combining the results of individual scorers [18]. The research altered an inexpensive and lazy strategy with multiple sites for searching for threats. According to Habibzadeh, smart city applications can create weaknesses in security [19]. Furthermore, removing weaknesses in security required the participation of both governmental and technology objects. Smart cities could be regarded as an instance of security. Said and Tolba developed a deep learning algorithm to forecast the efficacy of IoT communication networks using an adaptive neural net methodology for accomplishing forecasting procedures [20]. They discovered that the approach was having a considerable beneficial effect on sustaining smart cities and avoiding IoT network faults. Khan and others proposed a deep learning-based solution for transportation data projection and integration [21]. The findings revealed an improvement in precision, duration, and mistakes. Ghiasi and others investigated the Hilbert-Huang shift method for identifying fake data insertion attempts on the small scale [22]. The work they conducted relied on blockchain database technology and the study of electricity and electricity signals in sensors. Researchers discovered that the suggested approach might improve data interchange confidentiality in the network while also providing a more precise and reliable identification mechanism.

Other researchers used a combination of a singular value decomposition and two-dimensional Fourier transforms to identify the indices of the switching surface in sliding mode controllers [23]. They additionally tested the suggested approach in several bogus information attack vectors. Studies have demonstrated that the suggested approach can shorten the identification duration of an assault. In addition, the technology they used detected attempts with 96% accuracy. The authors studied electrical system resiliency principles by introducing assessment features [24]. They also developed an optimal configuration for robust power plants in the Noorabad system. They employed the grey wolf algorithms to discover the best grid settings. The results showed that both the suggested approach and the offered modification could increase efficiency and lower grid expenses.

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chişinău, Moldova

SMART CITIES AS A CYBER CRIMES TARGET

Cities have grown more intelligent and technologically advanced in the past few decades. Recent advances in technology, in addition to quick and easy interaction, allow cities to utilize more efficiently use their own resources, save finances, and provide excellent amenities to their inhabitants [25]. Cities' struggle for investment, new inhabitants, and visitors has increased emphasis on offering an excellent standard of existence and an exciting financial picture. Authorities have determined that, while budgetary constraints, inadequate funds, and outmoded processes often pose barriers to their objectives, emerging technology can transform these obstacles into possibilities. According to Chen and others, a smart city is one that employs an infrastructure to computerize and modify governmental processes in order to improve the lives of its residents [17]. Smart Cities improve technical infrastructure by increasing the efficiency and method of urban support, lowering financial burden and resource utilization, and interacting passionately and productively with residents. With the development of smart city technology, areas such as government functions and congestion, travel, water, power, wellness, and garbage disposal have grown by implementing Intelligent parking detectors, organized health monitoring, immediate noise in cities visualization, traffic management, sector optimizing, and automated illumination are examples of such devices based on the Internet of Things concept (IoT) [26]. Cloud computing, on the other hand, is an evolving framework for collecting and deciphering central smart city information [27].

Considering the essence of smart cities, it should be noted that urban smart design could incorporate mainly smart government, smart healthcare, smart energy and smart transport.

Smart government creates benefits for long-term social output by utilizing information and communication technologies for organizing, administration, and activities at one or multi-layer levels. In a nutshell, the deployment of company procedures that utilize technological innovation in intelligent administration promotes data continuity with management and the supply of exceptional services. The following phase in e-government is smart governance able to reduce crime by boosting the state of mind, enabling a rapid and effective reaction to incidents, researching situations, and enhancing public services [28].

Smart healthcare is a healthcare system which links individuals, medical centers, and organisations by utilizing technology like wearables, the Internet of Things, and mobile devices to constantly obtain data which proactively controls the environment's demands and reacts more intelligently [29]. Medical professionals, patients, healthcare facilities, and scientific institutions are the fundamental parts of smart healthcare. Infection avoidance, tracking patients, diagnosis and therapy, administration of hospitals, wellness choices, and research in medicine are all aspects of smart healthcare. Simply linking smart gadgets to medical facilities and statistical platforms allows for surveillance from afar.

Smart energy management was formed as a result of the inability of conventional power distribution networks to meet the rising needs of populations. A smart and contemporary electrical infrastructure is required to meet the demands for stability, scaling, control, sustainable energy output, and affordability [30]. A smart energy infrastructure having technological innovations may facilitate two-way exchanges of information and currents of electricity via network units. The smart grid allows for continuous evaluation, assuring the energy transfers across the energy network and customers are optimized and additionally allows for the generation of green energy by incorporating sources of clean energy into the electrical system (on the part of both the Power Company and the consumers.

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

Smart transport makes the best use of current infrastructure and advances in technology to boost network effectiveness while also increasing automobile and passenger security and decreasing time spent travelling. To attain that objective, transportation infrastructure requires effective structures that benefit the transportation industry, as well as adequate oversight of those networks [31]. The most significant benefits of implementing smart transportation systems are reduced congestion in traffic, greater security, savings in time, decreased emissions, and improved service. This technology's important components include infraction tracking and storage frameworks, a weather condition database, a driver alert mechanism, and an automobile data scheme, as well as the convenience of rapid and accurate investigations and increased welfare benefits.

CYBER SECURITY ASPECTS IN SMART CITIES

Cities have to embrace modern technological innovations in order to get sophisticated. Each emerging technology or metropolitan infrastructure provides cyber criminals with a fresh opening. For instance, in smart roadway management infrastructure, many connections across traffic controllers and lights occur sans encoding or verification, enabling an intruder to manipulate or falsify input [32]. Denial of service via channel gridlock, mathematical floods of devices that has limited power consumption (such as smart meters), a global denial of service to a city network, or postponing a time-critical communication that can lead to prevalent interruption is one of the most serious smart grid incidents. Fraud of information from different detectors is an additional concern in the metropolitan environment; for instance, forging devices to identify floods, quakes, assaults, and other natural disasters can result in erroneous warnings and public fear. An intruder spying on personal information transmitted through an intelligent structure to a meter with sensors poses a serious threat to user confidentiality. Furthermore, a hacker fabricating an individual's persona in order to remotely manipulate construction machinery can result in a variety of losses to the user.

The smart grid's reliance on the data system undoubtedly opens itself with potential connectivity and grid technology weaknesses. Grid management systems in older electrical networks were maintained segregated to insecure settings like the Internet. Cyber assaults on the electricity network are nevertheless readily taken through the context of smart grids from various elements of the network. An intruder, for example, is not required to gain entry into protected installations or equipment (such as generators, substations, command centers, and so on) to disrupt the electric power distribution chain. A threat may conduct an assault at every point on a smart grid [33]. Illegal network penetration could result in a wide range of negative effects on the intelligent grid. These repercussions involve customer data leaks, breakdown cycles that result in major interruptions, and generating and infrastructure downtime. The smart transmission grid is a collection of cutting-edge innovations that aim to upgrade the electrical supply network by incorporating information and communication technology. The data storage architecture for smart distribution networks is made up of computer programs and datasets. To perform effectively and manage, smart grid data center applications have to interact with one another. Thousands of important pieces of technology are employed in smart grids, and all of these devices are linked to smart city networks.

Data theft is one of the most serious security issues related to smart buildings. User confidentiality is a major issue in the age of smart grids and to improve safety, operation and customer benefits, high-energy user electrical usage data is transferred from

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

consumers' smart meter systems to various smart grid organizations which compromises user confidentiality [34]. Private data concerning the person such as their energy usage habits, the kind of electricity used, when the facility is vacant or full, and so on, can be revealed. Furthermore, traces left by battery purchases are able to be exploited by various organizations such as charging infrastructure as providers to gather information about electricity automobile use and setting, infringing on consumer confidentiality. Also, the assailant may get confidential data regarding the user and infringe confidentiality by spying. An additional threat of smart structures is communication modification or repetition - a criminal could put a sophisticated building's security at risk by altering or replaying messages about measurements could be altered. Because data from measurements is utilized for an array of functions accurate information tampering can result in loss of revenue for smart grid companies and weaken the reliability of the grid. An outsider could introduce updated usage signals or replay previous expenditure information of a gadget in a smart meter and bill the consumer for power not utilized. If necessary, the client sells power to the network by placing solar panels in the structure and also exports power against the intelligent grid in a crisis by employing an electric car to defend the grid against potential overloading failures. Each message delivered through the smart grid to an intelligent structure can be modified through an assail resulting in massive amounts of smart grid outages. Actual unscrupulous user may alter the email sent from the smart meters to the electrical provider including property usage statistics and reject payment for the consumption of electricity. Adjusting communications with flexible pricing communication from the energy sector to the client results in the client getting incorrect prices and making inappropriate decisions about when to use high-consumption appliances, thereby imposing an expense on the individual and putting more strain on the distributed energy system. Furthermore, a hacker may impersonate a smart meter and report erroneous quantities of energy used to the smart grid, as well as request/enter false power signs to be sent to sources of energy and electric automobiles, or obtain messages from the smart grid. The assailant can even pose as a client and remotely operate the electrical systems in the structure causing the consumer to make the remote control error and cannot operate the considered device when an intruder impersonates it [35].

MEASURES TO SECURE CRITICAL SMART CITY RESOUCES

The majority of programs for smart cities nowadays are supplied by electrical power. Lacking power, the majority of the smart city infrastructure and businesses will be unable to function, leaving the city in darkness. As a result, protecting power sources and delivering energy is crucial for smart cities. Electricity generation can be stopped by intentionally harming the location or by interfering with the production of the electricity process. That necessitates strong safety measures to ensure that power output is not disrupted and that backup power is available in the event of an outage. Energy shipment, on the other hand, refers to power communicated by cables, converters, relays that are toggles, and power stations. As a result, cyberattacks upon any of these parts can disrupt the supply of electricity, disabling all smart city operations. Hackers have been reported to be eyeing electricity-producing plants as probable targets for attacks in order to cause huge city outages and maybe spark mass uprisings [36]. It is critical to build an extensive scheme and structure for guaranteeing power production and electricity distribution to the metropolis. Moreover, because a power supply system is highly interconnected, a chain reaction of interruptions is possible, increasing the damage of one isolated attack. That can

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chişinău, Moldova

cause widespread outages across different places. To counter these kinds of assaults, smart towns must have included durability and separation capacity.

Communication is required for smart city facilities to link cameras, detectors, servers, and other devices. As a result, connection (together with energy) is an additional lifeline for smart cities. Connectivity can take place via wireless as well as wired networks. This might also be considered as IoT security. The device, data, and connectivity privacy are all aspects of IoT security. Safety for data is provided by encoding, while network privacy is achieved through the use of lightweight protection from beginning to end transportation protocols. Current communication networks that provide fixed high-speed internet or mobile cellular networks are fairly secure, with only a few instances of connection theft. Nevertheless, for a smart city, protection criteria ought to be increased since individuals want cities with sensors to be safer than regular cities.

Many smart city software may sense, obtain, procedure, and analyze information to produce meaningful knowledge, which will then be used to develop meaningful solutions. Smart transport applications will gather vehicle, traffic, and passenger data, whereas smart-health applications may capture individuals and doctor data. No matter what smart city applications are used, data will continue to be collected as part of the smart city system and must be protected, as well as in terms of its contents and its storage. This type of data can be safeguarded in numerous ways like access control entails preventing unauthorized access to data, cryptography techniques, identification, digital certificates, confidentiality etc.

According to the EU Agency for Network and Information Security, a list of best practices for the cybersecurity protection of smart cities has been identified [37]. They are:

- use of VPNs;
- encryption of data;
- use of network intrusion detection system;
- use of physical protection;
- install access control;
- install alarms and surveillance;
- implement security policy;
- creation of activity logs;
- maintenance of backups;
- regular auditing;
- shutdown procedures.

APPLYING DEEP LEARNING FOR CYBER SECURITY CHALLENGES

Deep learning is a subset of machine learning which focuses upon the research and construction of algorithms that learn systems [38]. Within simple terms, deep learning with data processing and similar to a human seeks out certain characteristics by itself, by means of a variety of sequential sections in its framework, with the aim to build a template for selection to resolve an issue. Because there are numerous levels to consider, deep learning can uncover specific elements that exist in each of them and use them to arrive at more informed choices when addressing the challenge. Deep learning is based on the continuous discovery and exploration of complicated databases. Learning is accomplished by constructing computer simulations known as neural networks, or neural networks, which are motivated by the inner workings of the human brain [39]. The system in question is divided into various operating layers. Deep learning attempts to take advantage of the undiscovered design in how inputs are distributed to try to identify suitable depictions

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

through an ordered arrangement of notions that correspond to the processing levels. Having learning from unmarked data input, deep learning may now generate additional data. As a result, it has been dubbed "innovative mind". Dispute-producing systems, for instance, one of the most common deeply creating models now, can generate images of outstanding quality, enhance the appearance of images, transform pictures to written form, and be utilized in security online to mimic attacks, help healthcare evaluate cancer via more genuine tests, and have employed in an assortment of additional limitless possibilities". It is worth noting that deep learning has joined the industry after the introduction of artificial intelligence. This learning process has aided machines with intelligence in responding more readily to human requirements and wants. Typical neural network types include multilayer and cyclic networks of neurons.

The first type is a deep learning technique that accepts a source image and allocates priority to every single object/aspect in the graphic to ensure they can be identified by one another. When opposed to other classifying methods, this technique involves lesser preparation. Whereas the primary approach to filtration is designed by hand, given sufficient instruction, a network of convolutional neural networks can acquire such filter/specifications [40]. The last kind is a sort of artificial brain network that is used for speech recognition, natural language processing, and sequencing data mining. Recurrent neural networks, compared to convolutional neurons, feature an adaptive loop whereby their output, in addition to each subsequent data, goes back to the network. Because of its inbuilt recall, a neural network with recurrent may remember its prior input and use it to process an ordered set of inputs. In terms of structure, these networks of neurons are made up of a cyclical loop that avoids prior data from being deleted and keeps it in the network.

Authorities are increasingly worried about security online in the last few years. It is a typical instance of how firms operating in the European Union (EU) have been compelled to follow tight EU standards, a method that has drastically decreased incidents of data theft. Methods using deep learning have a number of intriguing applications in smart cities. Without a doubt, a learning plan provides precise discoveries once outcomes of the entirety or comparable elements of the instruction and evaluation material are included. The second study area is knowledge disposal, which involves changing or transmitting the distribution of instruction and evaluation from a single system to another. Furthermore, researchers might look into incorporating linguistic networks into smart city applications to improve efficiency.

CONCLUSIONS

In this research, confidentiality and cyber-security in smart cities were investigated. The field of smart city network safety is nevertheless in its early days, with many rules, structures, goals, and technological advancements related to this critical subject. A review of the smart city security literature discovered that several studies provide useful assistance for politicians with city administrators seeking to more efficiently create and carry out smart city objectives and operations plans. Other research projects have outlined the conceptual framework of the deployment and evaluation of IoT in smart cities in order to give a framework for evaluating and testing proposals on a wide scale underneath real-world settings, but only a few have researched cyber security and confidentiality. People in the smart city noted an important research deficit in this field. Protection encompasses illegal data entry as well as actions, which interrupt accessibility to facilities. Considering the expansion of human populations and technological advancements in cities, sophisticated

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

methods of administration that leverage cutting-edge platforms and technologies in order to make urban infrastructure smarter are essential. Smart cities are an emerging form of technological and technological combination. The rate of assaults and vulnerability will rise as systems are linked and integrated. On the contrary hand, as additional information emerges involving the movements and behaviors of digital people, anonymity will become more insecure. As a result, it is critical to create strategies which concentrate on long-term cyberspace safety and danger reduction techniques. The analysis conducted in the current investigation revealed that overcoming these difficulties requires a great deal of administrations, software and hardware makers, and organizations delivering information technology safety services. Furthermore, creating adaptable systems with outstanding knowledge security capacities is critical to preventing major safety catastrophes, which can result in devastating monetary info, loans, including confidence losses. Because technological concerns or dangers to users' confidentiality are not just as significant in the context of smart cities, and relevant organizations and governments have a limited ability to react to their ears, further research should include an assessment and grading method.

BIBLIOGRAPHY

1. ALDAIRI, A., TAWALBEH, L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*. 2017, (109), 1086-109. ISSN: 1877-0509
2. ALIBASIC, A., JUNAIBI, R., AUNG, Z., WOON, W, L., OMAR, M., A. Cybersecurity for Smart Cities: A Brief Review. In: *Data Analytics for Renewable Energy Integration*. Riva del Garda, Italy, September 23, 2016, 22-30.
3. ARABO, A. Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science*. 2015, (61), 227-232. ISSN: 1877-0509
4. BAIG, Z., A., SZEWCZYK, P., VALLI, C., RABADIA, P., HANNAY, P., CHERNYSJEV, M., JOHNSTONE, M., KERAI, P., IBRAHIM., A., SANSUROOAH, K., SYED, N., PEACOCK, M. Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*. 2017, (22), 3-13. ISSN: 2666-2817
5. BJORNER, T. The advantages of and barriers to being smart in a smart city: The perceptions of project managers within a smart city cluster project in Greater Copenhagen. *Cities*. 2021, (114). ISSN: 1873-6084
6. CERRUDO, C., RUSSEL, B. Cloud Security Alliance. Cloud Security Alliance. 2015
7. CHATFIELD, A., K., REDDICK, C., G. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quaretrly*. 2019, (2), 346-357. ISSN: 1872-9517
8. CHEN, D., WAWRZYNSKY, P., LV, Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Societe*. 2021, (66), 2210-6715. ISSN: 2210-6707
9. CHEN, Z. Application of environmental ecological strategy in smart city space architecture planning. *Environmental Technology & Innovation*. 2021, (23). ISSN: 2352-1864
10. DEHDARIAN, A., TUCCI, C., L. A complex network approach for analyzing early evolution of smart grid innovations in Europe. *Applied Energy*. 2021, (298). ISSN: 1872-9118
11. DEHGHANI, M., NIKNAM, T., GHIASI, M., SIANO, P., ALHELOU, H., H., AL-HINAI, A. Fourier Singular Values-Based False Data Injection Attack Detection in AC Smart-Grids. *Applied Sciences*. 2021, (11).

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

12. FARD, S., M., H., KARIMIPOUR, H., DEHGHANTANHA, A., JAHROMI, A., N., SRIVASTAVA, A. Ensemble sparse representation-based cyber threat hunting for security of smart cities. *Computers & Electrical Engineering*. 2021, (88), 1879-0755. ISSN: 1873-2046
13. FENG, W., WEI, Z., SUN, G., ZHOU, Y., ZANG, H., CHEN, S. A conditional value-at-risk-based dispatch approach for the energy management of smart buildings with HVAC systems. *Electric Power Systems Research*. 2020, (188). ISSN:1873-2046
14. GHIASI, M. DEHGHANI, M., NIKNAM,T., KAVOUSI-FARD, A., SIANO, P., ALHELOU, H., H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access*. 2021, (9), 29429-29440.
15. GHIASI, M., DEGHANI, M., NIKNAM T., BAGHAEE, H., R.,PADMANABAN, S., GHAREHPETIAN, G., B., ALIEV, H. Resiliency/Cost-Based Optimal Design of Distribution Network to Maintain Power System Stability Against Physical Attacks: A Practical Study Case. *IEEE Access*. 2021, (9), 43862-43875.
16. HABIZAHEH, H., NUSSBAUM, B., H., ANJOMSHAA, F., KANTARCI, B., SOYATA, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Societe*. 2020, (50). ISSN: 2210-6715
17. HASBINI, M., AYOUB, R., TOM-PETERSEN, M., FALLETTA, L., JORDAN, D., SEOW, A., SINGH, S. Smart Cities Cyber Security Management. *Securing smart cities*. 2017
18. IJAZ, S., SHAH , M., A. KHAN, A., AHMED, M. Smart Cities: A Survey on Security Concerns, *(IJACSA) International Journal of Advanced Computer Science and Applications*. 2016 (7), 612-624. ISSN : 2156-5570
19. JEONG, H., H., SHEN, Y., C., JEONG, J., P., OH, T., T. A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications. *Vehocular Communications*. 2021, (31). ISSN: 2214-210X
20. KASHEF, M., VISVIZI, A., & TROISI, O. Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. *Computers in Human Behavior*. 2021, (124). ISSN: 1873-7692
21. KHAN, S., NAZIR, S., MAGARINO, I., G., HUSSAIN, A. Deep learning-based urban big data fusion in smart cities: Towards traffic monitoring and flow-preserving fusion. *Computers & Electrical Engineering*. 2021, (89). ISSN: 1873-2046
22. KHATOUN, R. S. Smart cities: Concepts, architectures, research opportunities. *Communications of the ACM*. 2016, (58), 46-57.
23. KOURGIOZOU, V., COMMIN, A., DOWSON, M., ROVAS, D., MUMOVIC, D. Scalable pathways to net zero carbon in the UK higher education sector: A systematic review of smart energy systems in university campuses. *Renewable and Sustainable Energy Reviews*. 2021, (147). ISSN: 1879-0690
24. LEBRUMENT, N., LEBRUMENT C., Z., ROCHETTE, C., ROULET, T. Triggering participation in smart cities: Political efficacy, public administration satisfaction and sense of belonging as drivers of citizens' intention. *Social Change*. 2021, (171).
25. LEE, K., SILVA, B., N., HAN, K. Algorithmic implementation of deep learning layer assignment in edge computing based smart city environment, *COMPUTERS & ELECTRICAL ENGINEERING*. 2021, (89). ISSN: 1879-0755
26. LI, P., LU, Y., YAN, D., XIAO, J., WU, H. Scientometric mapping of smart building research: Towards a framework of human-cyber-physical system (HCPS). *Automation in Construction*. 2021, (129). ISSN: 1872-7891

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

27. LIU, L., ZHANG, Y.Smart environment design planning for smart city based on deep learning. *Sustainable Energy Technologies and Assessments*. 2021, (47). ISSN: 2213-1396
28. MARAHATTA, A., RAJBHAMDARI, Y., SHRESHTA, A., SINGH, A., GACHHANDAR, A., THAPA, A. Priority-based low voltage DC microgrid system for rural electrification. *Energy Reports*. 2021, (7), 43-51. ISSN: 2352-4847
29. MARUF, M., H., HAQ, M.A., DEY, S.,K., MANSUR, A.A., & SHIHAVUDDIN, A.S.M. Adaptation for sustainable implementation of Smart Grid in developing countries like Bangladesh. *Energy Reports*. 2020, (6), 2520-2530. ISSN: 2352-4847
30. QUAYYM, S., ULLAH, F., TURJMAN, F.,A., MAJTAHEDI, M. Managing smart cities through six sigma DMADICV method: A review-based conceptual framework. *Sustainable Cities and Societe*. 2021 (72). ISSN: 2210-6707
31. RAZMJOO, A., OSTERGAARD, P.A., DENAI, M., NEZHAD, M., M., MIRJALILI, S. Effective policies to overcome barriers in the development of smart cities. *Energy research and social science*. 2021, (79). ISSN: 2214-6326
32. SAID, O., & TOLBA, A. Accurate performance prediction of IoT communication systems for smart cities: An efficient deep learning based solution. *Sustainable Cities and Societe.* 2021, (69). ISSN: 2210-6707
33. SENGAN S., VELAYUTHAM, P. RAVI, L., V. S., & V. I. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. *Computer & Electrical Engineering*. 2021, (91). ISSN: 1879-0755
34. TEMBLEY, M., ALSUMAITI, A., M., ALAMERI, W., S. Machine and deep learning for estimating the permeability of complex carbonate rock from X-ray micro-computed tomography. *Energy Reports*. 2021, (7), 1460-1472. ISSN: 2352-4847
35. THING, V. L.Cyber security for a smart nation. In *2014 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2015.
36. TOFT, P., DUERO, A., BIELIAUSKAS, A. Terrorist targeting and energy security. *Energy Policy*. 2010, (38), 4411–4421. ISSN: 1873-6777
37. V. S., K., PRASAD, J., & SAMIKANNU, R. Barriers to implementation of smart grids and virtual power plant in sub-saharan region—focus Botswana. *Energy reports*. 2018, (4), 119-128. ISSN: 2352-4847
38. VITUNSKAITE, M., HE, Y., BRANDSTETTER, T., JANICKE, H. Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*. 2019, (83), 313-331. ISSN: 1872-6208
39. WANG, W., HUANG, H., XIAO, F., LI, Q., XUE, L., JIANG, J. Computation-transferable authenticated key agreement protocol for smart healthcare. *Journal of Systems Architecture*. 2021, (118). ISSN: 1873-6165
40. ZHOU, X., LI, S., LI, Z., LI, W. Information diffusion across cyber-physical-social systems in smart city: A survey. *Neurocomputing*. 2021, (444), 203-213. ISSN: 1872-8286