RAS ENGINEERING & TECHNOLOGY

Research Article: Information Security Risks Valunerbility And Threat In Smart City Development In Africa

Issue Type: Volume1 Issue1

Author Name:
Dr. Yakubu Ajiji Makeri
Kampala International University
Uganda

Corresponding Author:
Dr. Yakubu Ajiji Makeri

Citation: Dr. Yakubu Ajiji Makeri Information Security Risks Valunerbility And Threat In Smart City Development In Africa

Received Date: 21st Nov-2020

Published Date: 3rd Dec-2020

Abstract:
Ongoing data innovations can encourage the change of customary regulatory cycles to administrations which can be performed on the web. The fast development of ICT ends up being lined up with its application for the fourth Industry Revolution. The worry and interest in data security are for the most part because of the way that data security hazard investigation (ISRA) is viewed as a central strategy not exclusively to distinguish and organize data resources yet in addition to recognize and screen the particular dangers that an association initiates; particularly the odds of these dangers happening and their effect on the separate organizations. Consequently, a sum of 18 years of research in Information Security was directed, and their discoveries were assembled and examined carefully. A large portion of the investigations was especially centering on investigating the different parts of security dangers and its countermeasure through exact explores, instrument improvement, deliberate writing audit, and dynamic examination affected from hypothetical information advancement to its usage development in Organization. Our surveys recommended that hazard investigation request basic and profound exploration to ensure they can present a powerful security countermeasure Our examination zeroed in on basic data framework, for example, Healthcare, Power System, and Manufacturing. One of the examinations, we applied exact investigation to order dangers and ascertain chances for the Healthcare framework. Notwithstanding that we created an apparatus utilizing Machine Learning to investigate different sorts of dangerous classes utilizing the equivalent dataset. In different cases, our exploration investigated data necessities required for SME based organization in executing hazard examination and conform to the standard. With similar destinations i.e., to present compelling security countermeasure, we investigated various techniques for breaking down dangers, weaknesses, and dangers utilizing endurance.

Keywords: Date security, Development, City

Introduction: The urban communities" are a popular expression existing apart from everything else. The lawful interest is developing, generally, scholarly reactions at any rate in the Africa, are still from the innovative, metropolitan examinations, natural and sociological as opposed to legitimate, sectors2 furthermore, have principally laid accentuation on the social, metropolitan, policing and ecological advantages of savvy urban communities, as opposed to their difficulties, infrequently a fairly uncritical fashion. Anyway, a developing reaction from the security and reconnaissance areas cautions of the possible danger to individual protection presented by brilliant cities . A central point of contention is the absence of opportunity in a surrounding or shrewd city climate for the giving of important agree to handle of individual information; other critical issues incorporate how much keen urban communities gather private information from inescapable public communications, the "privatization" of responsibility for foundation and information, the repurposing of "huge information"

drawn from IoT in savvy urban communities and the capacity of that information in the Cloud. Says Riaan Graham, deals chief for Ruckus Networks, sub-Saharan Africa: "The ICT area assumes a critical function in accomplishing this – availability implies residents approach data, information to improve, work together contrastingly and so on at the end of the day assemble an information-based and socially associated network. Information is as of now pricey which cutoff points access. This directly affects organizations, particularly SMEs that can't manage the cost of it, understudies who need admittance to data for instructive purposes, and simply typical residents that need admittance to embrace their day by day commitments. This is the reason we are seeing activities whose principal objective is to give free Wi-Fi to networks going to the front – all with an end goal to give unlimited availability to those that truly need it." Getting associated … truth be told, as urban areas get more brilliant, they remember one unavoidable truth immediately: any old Wi-Fi innovation won't cut it. Keen city applications request a remote organization that can manage intense issues like a complex cross-section in open-air conditions. To start with, I sketch the ascent of urban communities universally, both in the West and East and the less created South, and examine the key innovative, monetary, and political drivers which have made them a relentless portion of things to come metropolitan day to day environments of a great part of the worldwide populace. Instead of giving one formalistic meaning of savvy urban areas which will definitely be a moving target and may not help the lawful investigation, I attempt to draw their key attributes, zeroing in on two which are plainly risky from a protection outline: first, their reliance on mechanical frameworks, large information, the IoT and the Cloud; and second , their financing and henceforth "possession" in practically all cases by open private associations (PPP). Second, I spread out the notable weakness of urban areas, alongside different scenes for implanted IoT frameworks, to security dangers and how this is drawn nearer by the law in the EU. This segment makes very much trampled progress and is in this way generally short. It should be noticed that contemplations of "protection" (wrongly so named and restricted) in brilliant urban areas regularly stop here.

1. I go to more extensive issues of applied protection law structures, and spread out what might be seen as a fundamental hidden hypothetical issue, ie, that savvy urban areas are, generally, public places while generally security laws, for example, workmanship 8 of the European Convention on Human Rights (ECHR) and US security misdeeds have applied to private "air pockets" or zones zeroed in on the body, the home, and private interchanges. Drawing on ECHR case law just as attitudinal research, I contend sensible desires for security even in broad daylight spaces, as in savvy urban areas, are presently both perceived by European law and required by metropolitan occupants.

2. in the most pivotal part of the paper, I address in some detail the three key dangers to security and DP previously distinguished – the IoT, Big Data, and the Cloud - and plot how each issue shows itself to imperil the security of brilliant city inhabitants and clients. In every subsection I at that point attempt quickly to investigate how, and how well, EU DP law at present arrangements with managing, forestalling, or fathoming these dangers.

As the innovation and organizations become progressively incorporated, there is likewise the potential that this will uncover more weaknesses in mutually dependent frameworks that cybercriminals may hope to target. By abusing any such weaknesses in the organizations and programming of such mutually dependent frameworks, assailants could take data identified with private people – information vital to the consistent combination and activities of brilliant administrations – or in any event, cut down total tasks of keen administrations, which can prompt a technogenic catastrophe," says Badenhorst. Increasingly, we live in urban areas. Over the most recent twenty years, metropolitan focuses have become the objective of decision for residents and organizations looking for flourishing, soundness, and social and instructive offices, prompting the reformist relinquishment of country territories and the rising convergence of populace inside metropolitan regions. Over a large portion of the total populace as of now lives in urban areas: by 2050, 66% of the total populace is required to live in metropolitan zones, with almost 90% of that increment in Asia and Africa.

This urbanization cycle has become so noticeable that in a few states (eg, South Korea) the capital city produces as much as half of the nation's GDP: urban communities are hence at times turning out to be viewed as more significant than the nations in which they are located. Public governments frequently now set up services for urban areas (eg, in Brazil, India, UK) while nearby city chairmen, initiating city redevelopment and extension, have gained huge standing and worldwide notorieties in urban communities like London, New York, Barcelona, and Rio. Be that as it may, urban communities carry with them genuine difficulties. Around the world, high metropolitan thickness appears definitely to lead to issues including gridlock, energy gracefully and utilization issues, heightening of ozone-depleting substances emissions , spontaneous turn of events, absence of fundamental administrations, sensational increment in garbage removal needs, and expansions in wrongdoing and withdrawn behavior. The political also, social need to battle these issues (specifically, the ascent of natural worries, as environmental change stresses become ever-present), joined with the undeniable potential for a worthwhile market for innovation and broadcast communications organizations creating computerized and organized arrangements (for example IBM13, Cisco14, Vodafone15), has offered to ascend to the trendy expression idea of brilliant cities16

Yet, urban areas carry with them genuine difficulties. Internationally, high metropolitan thickness appears unavoidably to lead to issues including gridlock, energy gracefully and utilization issues, heightening of ozone-depleting substances emissions, spontaneous turn of events, absence of essential administrations, emotional increment in garbage removal needs, and expansions in wrongdoing and solitary behavior. The political furthermore, social need to battle these issues (specifically, the ascent of natural worries, as environmental change stresses become ever-present), joined with the conspicuous potential for a rewarding business sector for innovation and media communications organizations creating advanced and arranged arrangements (for example IBM13, Cisco14, Vodafone15), has offered to ascend to the popular expression idea of savvy cities . This thought has been hence anxiously jumped on by public and metropolitan political pioneers, major worldwide tech partnerships, and global establishments and associations the same (for example European Commission, OECD18, ISO19) . Kitchin depicts savvy urban communities as an endeavor to illuminate the principal problem of urban communities – decreasing expenses and making monetary development, while simultaneously creating maintainability, investment, a satisfactory norm of community administrations and personal satisfaction - yet cautions that there are various originations of brilliant urban areas and that a neo-liberal, market drove, technocratic point of view will in general rule, as contradicted to an elective worldview, which is to consider savvy to be as "resident-driven", encouraging social advancement, equity and commitment in what he terms a "brilliant society". Such strength by the unadulterated monetary increase viewpoint might be harmful to the thought of both social requirements and suitable legitimate guidelines, something which is starting to stream through as a worry in European arrangement hovers, despite the general "determinedly positive21" talk around brilliant cities . There is presently no single acknowledged meaning of a "shrewd city" also, much relies upon who is providing the attributes: industry, lawmakers, common society and residents/clients are four promptly and dissimilar arrangements of partners. It is simpler maybe not to characterize savvy urban areas yet to expand their key highlights. The interlocking key foundation that is frequently referenced as making urban communities "shrewd" incorporates:

1. Organizations of sensors joined to certifiable articles, for example, streets, vehicles, fridges power meters, homegrown apparatuses, and human clinical inserts which interface these items to advanced organizations (the "Web of Things"(IoT), "omnipresent registering" or ubicomp, or as Greenfield calls it, "Everyware"26). These IoT organizations produce information in especially colossal sums referred to conversationally as "large information" (see underneath).

2. Organizations of advanced correspondences empowering ongoing information streams which can be joined with one another and other and afterward be dug and repurposed for helpful results;

The cases made for urban areas in their publicizing and comparable promotion vehicles are significant both in their recognition and execution. Keen urban areas are said to "interconnect individuals, information, things, and measures under a powerful worldwide foundation". Brilliant urban communities at that point use this organized foundation all together "to improve monetary, asset, and political effectiveness while empowering social, social and.. metropolitan turn of events." As Bob Pepper, VP of Global Technology Policy for Cisco (a main savvy city merchant) put it: "What makes a city brilliant is that it perceives the centrality of innovation and data to improve its processes. These viewpoints are frequently utilized in similar investigations as markers depicting how "savvy" metropolitan territories are, to rank urban areas, regularly in a financing setting. For example, concurring to the 2015 Juniper Research report, Barcelona is right now at the first spot on the list of "shrewd urban communities", because of its sweeping utilization of new advances, including a keen traffic signal framework which sets the lights at green until fire motors have passed, crisis reaction gadgets introduced in the person's home and associated through a (land or cell phone) line to a Call Center, which can be reached at the basic press of a catch, and other innovations. New York City, London, Nice, and Singapore right now balance the top five.This positioning, has become fundamentally significant lately in driving future city improvements and ventures by both government and industry; "insightfulness" has become a serious file among urban communities for consideration, financing, and internal speculation. Keen urban communities are, in like manner, a worldwide social, financial, and political, just as a mechanical marvel. In the grew north, urban areas will, in general, be "retrofitted", or reflectively reevaluated as "savvy", to meet ecological, social, political, or business targets. In the UK, savvy urban areas are as a rule effectively advanced by the state utilizing interest in "keen city demonstrators" set in different urban areas, and through organizations, for example, Innovate UK (earlier NESTA), BIS (the administration service for exchange and industry), a state-supported "computerized launch" worth £50m, and a 2015 £40m IoT activity - all advocated by the expectation that the UK will turn into a world chief in this field, capable "to exploit up to a $40 billion portion of the [£400 billion global] commercial center [for shrewd cities] by 2020". In 2013, Glasgow, Scotland won a £24 million award as shrewd city demonstrator, and utilized the assets, expanding on a few existing frameworks, to build up a progression of activities, including shrewd streetlamps that light up when people on foot and cyclists are close and faint if there is less movement; an organization of sensors introduced under streets creating information which permits customizable traffic signals

to lessen gridlocks; a cutting edge "brilliant CCTV" control focus; and an "information vault" of open metro information which can be misused by scholastic specialists. Therefore it was asserted that "worldwide praise" came as a Geospatial World Excellence Award "for giving administration in exhibiting how more seasoned, more settled urban areas can be changed into Smart Cities of things to come". 38 Smart urban areas are subsequently not simply an issue of creating less contaminated or more proficient urban areas, yet produce significant political capital and large business openings alongside a huge potential fare market. In the creating scene, keen urban areas are similarly politicized however regularly assume an alternate part, of empowering modernization and advancement, reacting to issues emerging from populace pressure, environmental change, movement, and rustic to metropolitan progress. Non-Western savvy urban areas are frequently made without any preparation "top-down" instead of retrofitted. India for instance has pledged to make 100 new brilliant urban areas , distributing £760m to the project. Most such advancements are motivated by the "worldwide east" (eg Japan, Singapore, Korea): Africa is up 'til now not generally on the brilliant urban areas map, however, there are improvements in, eg, South Africa. Agricultural nations brilliant urban areas pull in an alternate arrangement of reactions, that they are vehicles for making gated shrewd areas of advantage, in an ocean of millions of innovation denied poor, are regularly settled by obligatory and questionable land procurement policies. Brilliant city financing is huge. Verifiably, especially in Europe, budgetary help from the money-stricken post-downturn public area, at the either public or metropolitan level, has not for the most part been adequate to back the revolutionary innovative organizations included.

Smart Cities: Security and Privacy

The urban areas are not a panacea for all ills, and they bring their own issues. A few, as of now noted, spin around useful issues, for example, financing, limit, admittance to pertinent innovations, interoperability of information, specialized normalization, and so forth Others are political: purchase in by the public furthermore, neighborhood legislators, the energy organizations, and the residents themselves – an ongoing NESTA report, looking over various urban areas, focuses that many shrewd urban areas "have neglected to convey on their guarantee, conveying significant expenses and low returns.. 'Brilliant urban areas' offer sensors, 'large information' and progressed processing as answers to these difficulties, however, they have regularly confronted analysis for being excessively worried about equipment instead of with people". Two further issues are especially apropos to this paper arranged for what it's worth in law: security, by which I mean the weakness of information to either coincidental or think penetrates because of specialized or authoritative disappointments; and security, in which I incorporate the European information insurance (DP) feeling of the privilege of people to control the assortment and preparing, including further re-utilizes, of their information. Security is likewise emphatically represented in Europe by the workmanship of the European Convention on Human Rights which goes about as a benchmark against which both EU DP rules and country state laws can be judged. Security and weaknesses Urban communities and their foundation are now the most perplexing structures ever made by men, and intertwining them with similarly complex keen urban communities arrangements, dependent on remote sensor networks and incorporated interchanges frameworks, makes them incredibly defenseless against power disappointment, programming mistakes, and digital assaults. Even a basic bug can hugely affect the metropolitan foundation.

The weakness and weakness of brilliant city frameworks is an ordinarily recognized phenomenon66, which echoes, and generally gets from, the notable absence of security and reliability of the IoT as a rule. The FTC in its powerful 2015 report on the IoT, notes security chances as its most noteworthy concern, both regarding the weakness of IoT gadgets themselves, prompting their trade-off or disappointment, and their expected use to spread weaknesses through networks and to different frameworks (the "zombie" problem). For instance, possibly, your keen, Web associated, refrigerator may be captured to send spam. The FTC has just taken its first requirement activity against a weak shopper IoT execution: an organization making child screens appended to the Internet, along these lines permitting guardians to see live feeds of their babies from a separation, had its feeds "hacked" in almost 700 cases. Associated vehicles (or "independent vehicles") are another critical IoT use situation where weakness to outcast hacking has as of now been illustrated: eg, Wired revealed in June 2015 how Jeep Cherokees could dependably be "commandeered" by outside programmers while on the road. Earthy colored, in a 2015 report for the ITU, take note of that "electronic assaults can.. lead to dangers to actual wellbeing" referring to potential targets, for example, clinical pacemakers, insulin siphons, and the vehicle slows down, and noticing the opportunities for criminals to spot "savvy metered" premises as presently unoccupied. These concerns just grow as the number of associated savvy objects develops. Cisco eg anticipate that there will be 50 billion gadgets associated with the Internet by 2020. For what reason is the IoT so unreliable? IoT gadgets, being, generally, little, modest, without an autonomous power source and produced in their millions, and truly for modern not purchaser use, are regularly planned with helpless encryption quality and an absence of other security features. The IoT vigorously depends on remote interchanges conventions or APIs that, because of the absence of obligatory specialized and security norms, are generally "just made sure about as a bit of hindsight, or more awful, not made sure about by any means, communicating information in the clear."The FTC report on IoT noticed that organizations making IoT gadgets might not have involvement with managing security issues; that they have regularly been considered as expendable; that fixing of weaknesses might not have been visualized .

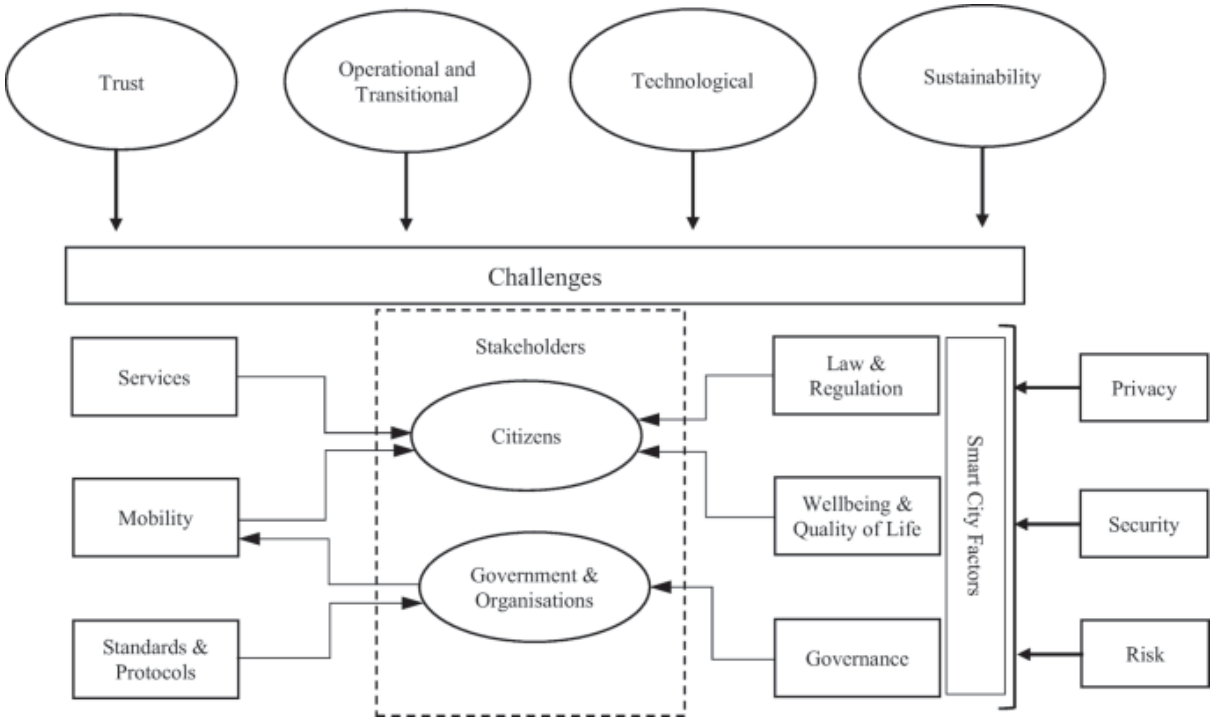

Figure1. Smart city privacy security framework

Privacy and Security of Mobile Devices and Services

Mobile devices are the backbone of interacting with the smart cities network infrastructure but present new challenges to the security and privacy of users where sensitive data could be vulnerable to attack by third parties. The Abi Sen et al. (2018) study proposed the use of fog computing properties such as caching, cooperating, and acting as a broker between users and the use of the cloud to mitigate security threats. The study presented three novel approaches for satisfying the required privacy of mobile devices within smart cities. The first approach utilized the concept of foggy dummies to protect the privacy of the user; the second incorporated a blind third party where a trust relationship is developed to protect the user from the server provider; the third approach used the concept of a double foggy cache to solve the trust issue between peers with a traditional cooperation approach. The Abi Sen et al. research posits the advantages of these approaches where there is no requirement to trust the party fully. The authors assert there is less overhead when compared to private information retrieval and the service provider cannot collect data on behavioral aspects of the user.

Privacy-preserving authentication (PPA) protocols for mobile services have emerged as a promising cryptographic approach to provide authentication and privacy protection features for smart cities. The research presented in Li et al. (2019) analyzed the PPA protocol suitability for mobile services within a typical mobile service application in a smart city context. The research findings outlined the efficiency of PPA when compared to other competing protocols, demonstrating that the proposed PPA protocol would exhibit less computation and communication overheads when deployed in mobile service applications for smart cities.

Smart City Infrastructure

Many articles focused on smart city infrastructure and ways to overcome security and privacy issues within smart cities (Abosaq 2019; Ainane et al. 2018; Alandjani 2018; Antoine Picon 2019; Awad et al. 2019; Baryshev et al. 2016; Bernardes et al. 2018; Chatterjee et al. 2017; de Amorim et al. 2019). The IoT plays a pivotal role within the infrastructure of smart cities as it provides the network architecture responsible for gathering and processing data from distributed sensors and smart devices. Studies generally categorize attacks on IoT devices into external and internal - attacks (Alromaihi et al. 2018; Mo et al. 2010).

The vulnerability of IoT based applications is directly related to the network paradigm where physical objects such as sensor-based devices collect data on key interactions within the network and communicate via wireless or wired connections. The data which is uploaded, processed, and stored can exhibit key vulnerabilities in the form of man-in-the-middle attacks and denial-of-service attacks. As a result, collecting and transferring data via the use of IoT infrastructure could severely impact the security and privacy of smart cities unless precautionary measures are implemented (Awad et al. 2019). Studies have argued that privacy can be easily compromised due to the high levels of interaction between people, devices, and sensors, thus highlighting the need for this data to be fully protected (Antoine Picon 2019; Elmaghraby and Losavio 2014). Studies have posited the merits of a more strategic focus on smart city security looking beyond aspects of data privacy toward a smart securitization policy (Efthymiopoulos 2015). The study by Ferraz and Ferraz (2014a) argued that information security does not only include privacy, confidentiality, integrity, and availability, but also includes interoperable security that represents the idea of a general failure of the urban system.

Protocols to Improve Security and Privacy

As smart cities face some challenges connected to security and privacy, some studies proposed various frameworks, models, and algorithms to improve these issues (Al-Dhubhani et al. 2018; Antonopoulos et al. 2017; Avgerou et al. 2016; Beltran et al. 2017; Burange and Misalkar 2015; Cagliero et al. 2015). This aspect of the literature has focused on encryption algorithms to build in security to smart city systems. The Antonopoulos et al. (2017) study tests high-level security feature algorithms by using Wireless Sensor Network (WSN) development. Stromire and Potoczny-Jones (2018) proposed to integrate an end-to-end cryptography system into smart city solutions at a foundation level. During any data breach, nothing about the data would be revealed by applying this system. Similarly, Lai et al. (2017) used an encryption approach in proposing a scheme titled Fully Privacy-Preserving and Revocable Identity-Based Broadcast Encryption (FPPRIB). The proposed scheme aimed to preserve the data privacy and the identity privacy of the receiver as well as the revoked user. The data can be securely protected and only the authorized user can access the data. The revocation process does not reveal any information about the data contents or the receiver identity and the public learns nothing about the receiver identity and the revoked user identity. These properties lead to applications in the smart city where identity privacy is desirable. The study by Patsakis et al. (2015) developed a cryptographic protocol that manages the huge amount of personal information that could be generated through e-participation in a scalable, interoperable manner, which guarantees the privacy of citizens within smart cities.

Network access control plays an important role in any communication system. It is important to develop adequate security of IoT system access to prevent any intruder from taking control of IoT devices or disclosing confidential information stored at the object or node level. Beltran et al. (2017) introduced SMARTIE, an integrating platform for user-centric secure IoT applications. It preserves user privacy while guaranteeing scalability and efficiency. The proposed platform efficiently provides decentralized access control for IoT devices based on user privacy preferences. SMARTIE aims to facilitate the integration of user-centric privacy and governance within IoT applications in a scalable and efficient mode. The authors highlighted that the proposed application will allow users to control their devices that join the application in terms of sensing and publishing data and enable fine-grained access control rules for their devices whilst deciding who can and cannot have their device data. The solutions proposed by Burange and Misalkar (2015) and Peters et al. (2019) mitigate privacy risks by providing the final decision maker with the opportunity to finalize network access for the client thereby protecting the privacy of user data. The Peters et al. (2019) study proposed a privacy awareness framework - PrivacyZones, which requires the service provider to share meaningful features of the data collected by their application. The proposed framework was successfully tested using two case study services (Hail-A-Taxi and Get-A-Discount).

Conclusion

Use of AI can improve security and privacy in smart cities. González García et al. (2017) proposed and tested the analysis of pictures through computer vision to detect people in the analyzed images. By using different tests, it was found that the system detects pictures with heads and shoulders more accurately in comparison with other images. Additionally, the study found that it is possible to integrate computer vision within IoT networks and that pictures can be used as sensors thereby, helping to improve the security of homes within smart cities. Huerta and Salazar (2019) proposed a framework by using AI and cognitive functions, which are capable of learning to understand, analyze, and audit every product in an automated intelligent manner.

References

1. Nicholas Nhede has been writing for Smart Energy International's print and online media platforms since 2015. He also contributes to Clarion Energy's other energy publications, including Power Engineering International and ESI-Africa.

2. See Roberto De Bonis and Enrico Vinciarelli, From Smart Metering to Smart City Infrastructure. Could the AMI Become the Backbone of the Smart City?, Smart 2014: The Third International Conference on Smart Systems, Devices, and Technologies (2014).

3. White Paper The Internet of Things. How the Next Evolution of the Internet is Changing Everything. Cisco white paper (2011), p. 3, at http://www.iotsworldcongress.com/documents/4643185/0/IoT_IBSG_0411FINAL+Cisco.pdf

4. According to the HP Fortify report, 70% of most commonly used IoT devices contain security vulnerabilities, including password security, encryption, and a general lack of granular user access permissions. See HP Fortify, Report Internet of Things Research Study (2014), p. 5, at http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

5. Akamai, akamai's [state of the internet] report (2014), p. 1, at https://www.antel.com.uy/wps/wcm/connect/2e38bd0047ad6c9682d3e7af6890d810/q3-2014-state-of-the-internetreport+(2).pdf?MOD=AJPERES

6. Supra n 65 at p 13. 76 See Kevin Tofel Got an IP webcam? Here are 73,000 reasons to change the password GigaOm Research, 7 November 2014 at https://gigaom.com/2014/11/07/got-an-ip-webcam-here-are-73000-reasons-to-change-from-thedefault-password/

7. See Cesar Cerrudo, Hacking US (and UK, Australia, France, etc.) Traffic Control Systems. IOActive (April 30, 2014), available at http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html

8. The term seems to originate from security researcher Tod Beardsley. See http://panelpicker.sxsw.com/vote/54858. More politely, Townsend predicts that smart cities may be "buggy,

brittle and bugged": see Townsend supra n 14 ch 9.
9. Antonopoulos, K., Petropoulos, C., Antonopoulos, C. P., & Voros, N. S. (2017). Security data management process and its impact on smart cities' wireless sensor networks. Paper presented at the South-East Europe Design Automation, Computer Engineering, Computer Networks, and Social Media Conference, SEEDA-CECNSM 2017,
10. Avgerou, A., Nastou, P. E., Nastouli, D., Pardalos, P. M., & Stamatiou, Y. C. (2016). On the deployment of citizens' privacy-preserving collective intelligent e-business models in smart cities. International Journal of Security and its Applications, 10(2), 171–184.
11. Babdullah, A., Rana, N. P., Ali, A. A., Dwivedi, Y. K., & Lal, B. (2017). Assessing Consumer's Intention to Adopt Mobile Internet Services in the Kingdom of Saudi Arabia. AMCIS 2017, Boston, USA, 10-12th August 2017.
12. Belanche-Gracia, D., Casaló-Ariño, L. V., & Pérez-Rueda, A. (2015). Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. Government Information Quarterly, 32(2), 154–163.
13. Bhati, A., Hansen, M., & Chan, C. M. (2017). Energy conservation through smart homes in a smart city: A lesson for Singapore households. Energy Policy, 104, 230–239.
14. Burange, A. W., & Misalkar, H. D. (2015). Review of the internet of things in development of smart cities with data management & privacy. Paper presented at the Conference Proceeding – 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015, 189–195
15. Chatterjee, S., & Kar, A. K. (2018). Effects of successful adoption of information technology-enabled services in proposed smart cities of India: From user experience perspective. Journal of Science and Technology Policy Management, 9(2), 189–209.
16. Chatterjee, S., & Kar, A. K. (2015, August). Smart Cities in developing economies: a literature review and policy insights. In 2015 International Conference on Advances in Computing, Communications, and Informatics (ICACCI) (pp. 2335–2340). IEEE.
17. Chatterjee, S., Kar, A. K., Dwivedi, Y. K., & Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Information Technology & People, 32(5), 1153–1183.