Research Article

open access

Citation date: 2019/12/01

Improving Security Performance in Smart Campuses

Musaab Mohammad Alhaddad

Director, IT Managed Services, Ericsson AB

How to cite:

Musaab, M, M "Improving Security Performance in Smart Campuses," *Res. Rev. Sci. Technol.*, vol. 1, no. 1, pp. 17–28, 2019.

Article history:

Received: 2019/07/21
Available online: 2019/12/01

Abstract

The idea of a smart campus is to combine devices, apps, and people to achieve enhanced operational and educational efficiency. One of the major aspects of the establishment of smart campuses is the building of a smart security system. This research is an effort to review the security technologies and how to increase the security performance of a smart campus using these technologies. The main objective of this study is to discuss asset security and facility access technologies in a smart campus setting. Universities spend millions of dollars on specialized equipment, yet maintaining track of such assets may be challenging. We discussed how security personnel can monitor the whereabouts of high-value items by installing IoT on them and how Smart locks, intelligent ID, and Geofencing can enable the facilities managers to manage campus access, tracking, and define zones. Finally, we review the optimal mix of other technologies and strategies to produce successful deterrent, preventive, protection, and reaction measures. This study argued that using these technologies smart campuses can alter the education system by improving campus security and by offering students and educators an engaged, creative, and safe environment.

Keywords: Asset security, Bacons, BLE, Smart campus, Smart locks

Declarations

Competing interests:

The author declares no competing interests.

Introduction

The Internet of Things (IoT) and other breakthrough technologies have allowed colleges and universities throughout the world to transition into digitally linked campuses that benefit students, staff, and the communities in which they are located. As a consequence, these contemporary campuses benefit from better student achievement and quality of life, as well as decreased operating costs, increased security and safety (Talei et al., 2015; Mattoni et al., 2016).

As with smart cities, smart campuses are characterized as locations where gadgets and software enable the creation of unique experiences or services and improve operational efficiency (Zhuhadar et al., 2017). Smart campuses may expand at a quicker rate than smart cities, since new generation students demand internet connection in their study and social contexts. The notion of implementing digital campuses is also embraced by the academic authorities who are always looking for new methods to enhance the academic and social experience of students while simultaneously reducing security concerns and lowering increasing running expenses. Municipalities and campuses have many of the same purposes. They are both aiming to appeal to people and investments in their towns and looking to build services and apps that enhance the experiences of citizens and students and make them safer (Yin et al., 2015). Additionally, they are attempting to separate out from the pack by exhibiting creativity and leadership.

A smart campus may aid in the improvement of three critical aspects: comfort, convenience, quality learning. It has the potential to transform how students' study, learn, and engage with an institution. And what knowledge they gain. It has the potential to be the spark for the transition that will allow universities to approach for the future of education and employment while changing the campus experience. It may continue to service the conventional campus as required while also allowing it to embrace new techniques to serve in the manner that its stakeholders have grown to anticipate. Universities, like other businesses that are embracing smart environments, serve their particular constituents in a comparable way. A smart environment allows smart campuses to supplement and coordinate with the broader smart environment plan, enabling campuses to maximize efficiency, nurture sustainability, and enhance the everyday circumstances for their constituents. As stated by (Abuarqoub et al., 2017), a smart campus seeks to enhance smart energy, water, and waste management. Environmental variables such as heat, humidity, pressure, and natural illumination have a direct influence on building energy use (Abuarqoub et al., 2017). For example, on campus, environmental sensors would regulate lights, turning them off on a regular basis if there was no activity in the space. Furthermore, smart grids will allow utilities or people to manage when devices are used, giving consumers more control over when and how much power they use. This is anticipated to balance the demand for peak electricity and distribute the load more uniformly across time.

Smart IoT technology may offer a diverse framework to promote all of aims of establishing a smart campus. By incorporating cutting-edge technology into the lifestyle of people, work and study on campus—and simply by having a digital platform that fosters innovation—educational institutions can improve their reputations for potential students and research programs. And, since all of those smart devices share a common technical backbone, educational institutions can benefit from new efficiencies fueled by big data and analytics and IoT integration as those technologies continue to develop (Muhamad et al., 2017) (Alhaddad, 2017, 2018b, 2018a).

Traditional campus security systems utilize access control systems, intruder alarms, panic buttons, and video surveillance (Garcia, 2003; Costomiris, 2018). However, in the majority of situations, these systems operate in technological silos, disconnected from one another and from other campus systems (Dong et al., 2020). By combining diverse security technologies into a cohesive system (Dutta et al., 2007), universities may achieve far more than the sum of their isolated parts in terms of safety and security services. Together, lighting, security cameras, alarms, and smart ID cards can now make automatic real-time choices that ensure safety for everyone on campus. University campuses already function as micro-societies in their own right as places of labor, residence, and recreation, there is great scope for campuses to allow smart city type change on a smaller scale.

Asset security

A campus asset is anything that has worth for a campus. What the utility is, such as a desktop, sporting equipment, automobile, dorm furnishings (Landsmark, 2011) (Harris, Boerger and Rimkus, 2014), and what shape the value is, relies on the organization and its members. Universities are accountable for handling a huge number of assets, facilities, and infrastructure. These resources may be placed in numerous locations at one campus or distributed out to different sites out of campus. Regardless of where these resources are situated, they ought to be monitored and maintained.

The university's physical assets comprise both fixed and flexible elements, ranging from underground utility distribution pipes to bench-top laboratory apparatus to flexible classroom furniture, chair and desks (Jiang, Xu and Zhang, 2012).

The whole system of asset monitoring at many university campuses has altered. To assist their students' achievement, higher education institutions are understanding that the supply of exceptional physical and online assets that fulfill the learning demands of their students would aid to secure the future of the institution. The assets supplied to employees, educators and students now a days go much beyond merely a desktop or a printer.

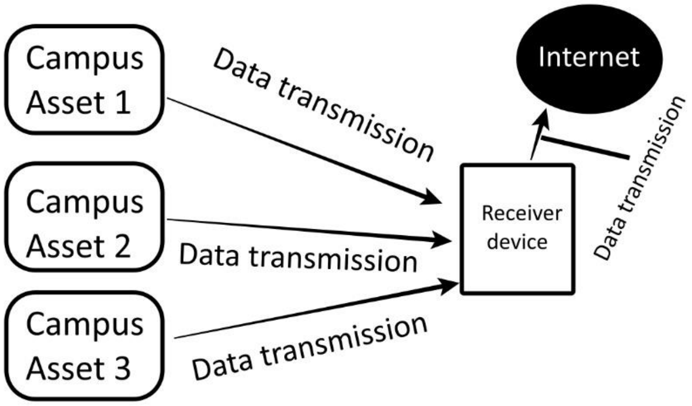
One of the fundamental tools for asset protection at smart campuses is the Bluetooth Low Energy (BLE) technology (Terán et al., 2017). It is a radio-frequency (RF) technology for wireless transmission that may be used to identify and monitor the location of people, devices, and assets for numerous indoor positioning use cases - such as asset tracking, indoor navigation, proximity solutions and more (Bisio, Sciarrone and Zappatore, 2016) (Han et al., 2015). Incredibly broad and approachable, Bluetooth is omnipresent across interior environments and accepted by many of today’s electronics.

Beacon technology utilizes Bluetooth Low Energy (BLE) to broadcast periodic messages (Palumbo et al., 2015). I t is because BLE is a low-power Bluetooth standard that was created for IoT based Applications and devices such as beacons (Zhuang et al., 2016). There are numerous considerations when developing such a system in smart campuses, from the back-end to the front-end, as well as mobile and incorporated application development, however this simple technique of tracking where moving assets in smart campuses travel and how long they stay in certain locations consumes very little bandwidth and is becoming increasingly affordable.

Chang (Chang, 2017) employed automated position recognition to develop a proactive guide system for museum visitors. There are three components of the system, namely, Beacons, a phone program, and a guidance control system. If Bluetooth is enabled, the notice is received by the visitor's smartphone, which assists the beacon in determining its position. Smartphones may be pushed with images, videos, text, music, and other multimedia to direct people to the next exhibit depending on their location.

Beacon tracking has a great number of possibilities for indoor location in smart campuses due to the higher demand and use situations for indoor tracking systems, as well as the lower activation costs. With the fast-expanding quantity of IoT devices - many of which include Bluetooth as a standard feature - the number of applications for this type of system is expected to expand significantly. The Bluetooth v5 benchmark is promising and significantly increased range, communication speed, and energy efficiency, among other features. It has been anticipated that the advancement and widespread application of this technology will accelerate for both of the Bluetooth applications, as well as for many more.

One of the primary needs for university infrastructure is that it should give a low-cost solution with the most possible functionality (Vafin, 2017, 2018). Bluetooth Low Energy is a wireless in-building technology that enables the development of a diverse variety of applications that make neighboring infrastructure more adaptable and intelligent.



Campus assets may collect measurements and transmit the information to a smartphone or laptop as shown in the figure 1. The cellphone or laptop can analyze the data, such as previous patterns, and notify the user if any metrics exceed the specified limitations. It may also communicate data to the campus's asset management staff through the Internet.

Control of facility access

Numerous university resident halls continue to use outmoded technologies such as conventional locks and keys. A single misplaced key has ramifications for security, time, and cost. Students, housing managers, and facility managers can get advantages from an access control system that incorporates smart locks.

Additionally, lost keys come at a high cost - both in terms of time and money. Student are urged to help who report misplaced keys. Additionally, residence directors must act immediately to change their keys. This procedure often includes rekeying locks, issuing new keys to, and verifying the process. Facilities employees must be sent to complete the repair, and extra staff must guarantee that students are compensated for their loss.

Thus, key loss is expensive in a variety of ways. There are direct expenses associated with key and lock renewal, but there are also indirect costs associated with having housing employees interrupt their usual job flow to respond to the replacement procedure. Facilities and residential units stand to save significantly by using a security system that does away with the need for conventional keys.

Smart locks have the potential to resolve the issues that households face. Smart locks may be opened without the need of keys and support a range of different entry methods. Students may access their buildings and room using codes, key cards, or a combination of these. They may even utilize an app to seek access as required with the proper integration.

Smart locks are connected to a smart phone which is used to regulate entry to the lock. As with other BLE devices, the controller (smart phone) may provide other users permanent or temporary access to the lock. As a result, phone serves as the key for smart lock. When it comes to smart locks, the primary worry of end users is security. Manufacturers of smart locks are cognizant of this and guarantee that buyers of smart locks get the optimal mix of security and ease. Smart locks are built with great accuracy utilizing a common lock mechanism. It is composed of two major components: hardware and software. The hardware and software are expected to operate in unison to guarantee the smart lock's optimal operation in the campuses' residents hall.

Bluetooth locks provide a variety of locking functionalities. It can detect when a student is near a specific distance and automatically unlock the door as he or she approaches then can unlock the lock by pressing phone or key fob on it. Bluetooth consumes less energy, allowing batteries to last longer.

Fingerprint entry may be quite easy, particularly for small campuses looking to guarantee that only authorized staff have access to locations containing sensitive data or costly products (Xavier, 2019). They are simple to program and often support many fingerprints. This strategy is most often used in workplaces. It enables doors to be unlocked with a key fob or a credit card. While the majority require pressing the fob/card against the RFID reader, some may be opened remotely.

Certain locking systems may be connected to a hub, enabling Wi-Fi communication and enhancing functionality. With a Wi-Fi-connected lock, staff of smart campuses can effortlessly monitor who opens and closes the door, when they do so, and even wirelessly lock the entrance from anywhere in the world with a cellular or wireless connection.

Unlocking the door with a keypad requires a pin number. They are simple to set up and allow for the creation of several pin codes for various users, as well as the ability to modify the pin code at any moment, making them ideal for campus administrators. When the study periods of a student ends, campus administrators can update the pin code to a new student staying on campus.

When used with home security systems, smart locks may significantly improve your campus' protection. Converting a campus into a smart campus, these smart locks allow users to connect the security system with other home systems, allowing them to even control or deactivate lighting remotely using their smart phones. For instance, when the front door of a classroom is secured using a smart phone, the lights are instantly turned down. By using smart locks in smart campuses, campus administrators will get a complete report on smart phone detailing the number of times it was book throughout the day and the individuals who accessed it. For instance, campus administrators may keep track of how often staff or students enters and exits an office or classroom.

Geofencing allows for the assignment of virtual limits to a physical geographical region in the actual world (Cardone et al., 2014). These virtual perimeters may be shown on an interior map and can be used to trigger actions or alerts upon entrance, exit, or residence inside the designated region.

Geofencing solutions make use of a variety of device detection mechanisms, including Wi-Fi, cellular, GPS, and RFID signals, to identify when a mobile phone or tracker tag approaches or departs a virtual border established around a given geographical area inside the covered facility (Rahimi, Nur Zincir-Heywood and Gadher, 2013; Oliveira et al., 2015). Geofences may be created in any form or size and are used to identify restricted zones or rooms with more restrictive restrictions. Within governmental and other high-security facilities, geofencing may generate alerts based on positional signals within these restricted zones, assisting staff in locating the event.

Although geofencing is most often mentioned in a marketing environment, the applications for these virtual barriers are many. Smart campuses may utilize interior geofences (Chen et al., undefined 2018) to track traffic inside a certain region of a building, making them an extremely helpful tool for anything from boosting security systems to improving workspaces.

Within institutions, geofencing and administration are critical due to the diversity of resources and unique configurations of the security and maintenance forces. While large institutions may be structured similarly to cities, with a police department committed only to responding to that community's needs, many companies, small campuses, and institutions will have smaller security teams. Which is why it is critical that geofencing technology aimed for these institutions be simple to implement and operate.

It is also important that system users have the ability to construct various geofences to account for different campuses or off-site locations. Each geofence may then be associated with a unique phone number and system user, ensuring that every emergency call is routed directly to the person or team allocated to respond to that area. For universities with several departments, buildings, and safety personnel responsible for dispatching depending on specified characteristics, the procedure might get fairly detailed (Petcovici and Stroulia, 2016).

Effective geofencing security methods need a few components. The solution will need on-premises equipment that is air-gapped from production networks. Sensors, switches and routers, Cat5 or Cat6 cabling, and a server to handle the software will comprise this equipment (O'Driscoll, 2014). After installing the solution, administrators set the indoor device detector to monitor and analyze a building's transmitting environment, allowing display of the radio frequency (RF) surroundings in the framework of a floor plan (Grayson et al., 2016).

Other technologies to improve security performance in smart campuses.

Interactive signage and kiosks.

Networked displays can transmit critical data during emergencies. A apps may route notifications to the appropriate displays depending on their location (Slack and Rowley, 2002).This technology can become developed into a vehicle for increasing awareness and involvement in smart campuses (Anirudh et al., 2017). While touchscreen displays may aid in general navigation, the addition of face recognition enables smart displays to tailor the interaction by greeting prospective students and directing them appropriately.

Intelligent locators.

Students may use smart pathfinding to plan the optimal way to their courses using their smartphone. If a student is concerned about going alone, especially at night, she may establish an alert that notifies trusted contact and campus police. If she does not appear at the specified time or does not turn off the alarm, those connections will be notified, fed her picture and personal information, and provided with her smartphone's exact geolocation for fast follow-up.

Management of parking, transit, and street crossings.

Drivers are directed to available parking places using parking sensors. Since drivers are less preoccupied when parking, the probability of collisions for pedestrians and cars both decreases. Collision warning technologies also assist shuttle drivers avoid accidents by supplementing their monitoring of blind zones (Chang, 2012). Additionally, crosswalks may use integrated LEDs that alter color and illuminate in response to the environment (Chandrika and Qureshi, 2018). If a walker is more focused on the device in his hand than on the automobile on the road and enters the crosswalk, red lights may flash to warn both parties of the hazard.

Push notifications and alerts.

While multi-modal notifications to the whole community are fairly frequent during an emergency, emerging applications may detect, target, and contact people who are directly in the line of damage or notify their presence during an emergency evacuation (Liu et al., 2017). Likewise, individuals with disabilities may utilize wearables to assist first responders in locating them during medical crises.

Intelligent lighting.

Smart nodes can control lighting settings and identify occupancy to distribute light exclusively to areas where individuals are located (Raza *et al.*, 2017). When bulbs are ready to break, smart lights can notify maintenance to the need for immediate replacement.

Surveillance video analysis on a huge scale.

While conventional closed-circuit cameras need wired connections and closeness to electricity, the linked campus may install small, intelligent IP video cameras nearly everywhere, with the video picture streamed over Wi-Fi for remote viewing by public safety personnel. Video analytics may be used to identify persons who are not members of the campus's official community or to count the how many people are walked by sensors at predetermined time intervals.

Conclusion

With the rapid growth of cloud technology, big data, and the Internet of Things (IoT), modern information technology is increasingly being incorporated into the education sector, resulting in a continuous improvement in the rate of university informatization. The security system structure of the smart campus campus network impacts the success or failure of establishment of smart campus and is one of the primary issues impeding smart campus growth. A smart campus enables supporting and engaging experiences via the deployment of modern network infrastructure and web gadgets. It connects individuals, devices, and applications and enables educational institutions to make informed choices about security and resource allocation. Smart campus administrators recognize the critical nature of implementing new technology and equipment in order to reduce operational expenses, and can thus provide customized solutions that result in energy savings and cost savings.

Research on smart campuses is currently more critical than ever due to the changing landscape of education sectors across the globe. This article examines a few instances of intelligent campus security construction. Such projects may assist educational institutions in improving the security, keeping up with developing technology and current events, and improving the overall user experience. However, the funding must be accessible in order to install the system in the first place. Numerous universities are recognizing the critical role that specialized private finance can play in assisting them in achieving their ‘smart' aspirations and adapting to quickly changing student and faculty expectations.

References

Abuarqoub, A. *et al.* (2017) “A Survey on Internet of Things Enabled Smart Campus Applications,” in *Proceedings of the International Conference on Future Networks and Distributed Systems*. New York, NY, USA: Association for Computing Machinery (ICFNDS ’17, 50), pp. 1–7.

Alhaddad, M. M. (2017) “The Impacts of EdTech Collaboration, IoT-Connected Classroom and Intelligent Grading System on Educational Performance,” *Advances in Contemporary Science and Technology*, 2(1), pp. 44–67.

Alhaddad, M. M. (2018a) “Artificial Intelligence in Banking Industry: A Review,” *ResearchBerg Review of Science and Technology*, 2(3), pp. 25–46.

Alhaddad, M. M. (2018b) “Implementing Blockchain in Public Sectors in MENA Countries: Opportunities and Challenges,” *Empirical Quests for Management Essences*, 2(4), pp. 30–45.

Anirudh, A. *et al.* (2017) “Next generation Indian campuses going SMART,” *International Journal of Applied Business and Economic Research*. researchgate.net, 15(21), pp. 385–398.

Bisio, I., Sciarrone, A. and Zappatore, S. (2016) “A new asset tracking architecture integrating RFID, Bluetooth Low Energy tags and ad hoc smartphone applications,” *Pervasive and mobile computing*. Elsevier, 31, pp. 79–93.

Cardone, G. *et al.* (2014) "Crowdsensing in Urban Areas for City-Scale Mass Gathering Management: Geofencing and Activity Recognition," *IEEE sensors journal*. ieeexplore.ieee.org, 14(12), pp. 4185–4195.

Chandrika, M. P. K. and Qureshi, M. A. S. (2018) "Comparison on Implementation Models of Smart Applications Using IoT Technology." academia.edu. Available at: https://www.academia.edu/download/57334671/IRJET-V5I837.pdf.

Chang, W. T. (2017) "Proactive guiding with iBeacon in art museum," *Annual Conference and Joint Meetings (PNC)*. ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/abstract/document/8203530/.

Chang, Y.-C. (2012) "Evaluation and Exploration of Optimal Deployment for RFID Services in Smart Campus Framework," in *Computer Science and its Applications*. Springer Netherlands, pp. 493–502.

Chen, L.-W. *et al.* (undefined 2018) "Smart Campus Care and Guiding With Dedicated Video Footprinting Through Internet of Things Technologies," *IEEE Access*. ieeexplore.ieee.org, 6, pp. 43956–43966.

Costomiris, R. (2018) "Campus Security During a Shooting." digitalcommons.georgiasouthern …. Available at: https://digitalcommons.georgiasouthern.edu/cgi/viewcontent.cgi?article=1640&context=faculty-senate-index.

Dong, Z. Y. *et al.* (2020) "Smart campus: definition, framework, technologies, and services," *IET Smart Cities*. Institution of Engineering and Technology (IET), 2(1), pp. 43–54.

Dutta, R. *et al.* (2007) "The SILO Architecture for Services Integration, controL, and Optimization for the Future Internet," in *2007 IEEE International Conference on Communications*. ieeexplore.ieee.org, pp. 1899–1904.

Garcia, C. A. (2003) "School Safety Technology in America: Current Use and Perceived Effectiveness," *Criminal justice policy review*. SAGE Publications Inc, 14(1), pp. 30–54.

Grayson, L. M. *et al.* (2016) "Accuracy of WAAS-Enabled GPS-RF Warning Signals When Crossing a Terrestrial Geofence," *Sensors* . mdpi.com, 16(6). doi: 10.3390/s16060912.

Han, G. *et al.* (2015) "Testing a proximity-based location tracking system with Bluetooth Low Energy tags for future use in the OR," in *2015 17th International Conference on E-health Networking, Application Services (HealthCom)*. ieeexplore.ieee.org, pp. 17–21.

Harris, J. S., Boerger, Z. and Rimkus, K. R. (2014) "Illinois Campus Media Census." ideals.illinois.edu. Available at: https://www.ideals.illinois.edu/handle/2142/58899.

Jiang, X., Xu, M. and Zhang, D. (2012) "Strengthen budget management, promote university's asset allocation," in *2012 International Conference on Information Management, Innovation Management and Industrial Engineering*. ieeexplore.ieee.org, pp. 450–453.

Landsmark, T. (2011) “Sustainability and Preservation in an Age of Campus Innovation,” *Planning for Higher Education; Ann Arbor volume*. search.proquest.com, pp. 51–54. Available at: https://search.proquest.com/openview/d56fa06bbafc49cd1f35868a7ae0982b/1?pq-origsite=gscholar&cbl=47536.

Liu, K. *et al.* (2017) “Location-aware smart campus security application,” in *2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. ieeexplore.ieee.org, pp. 1–8.

Mattoni, B. *et al.* (2016) “A matrix approach to identify and choose efficient strategies to develop the Smart Campus,” in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*. ieeexplore.ieee.org, pp. 1–6.

Muhamad, W. *et al.* (2017) “Smart campus features, technologies, and applications: A systematic literature review,” in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*. ieeexplore.ieee.org, pp. 384–391.

O’Driscoll, G. (2014) *Manage Your Smart Home With An App!: Learn Step-by-Step How to Control Your Home Lighting, Thermostats, IP Cameras, Music, Alarm, Locks, Kitchen and Garden with an App!* HomeMentors. com.

Oliveira, R. R. *et al.* (2015) “An intelligent model for logistics management based on geofencing algorithms and RFID technology,” *Expert systems with applications*. Elsevier, 42(15), pp. 6082–6097.

Palumbo, F. *et al.* (2015) “A stigmergic approach to indoor localization using Bluetooth Low Energy beacons,” in *2015 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. ieeexplore.ieee.org, pp. 1–6.

Petcovici, A. and Stroulia, E. (2016) “Location-based services on a smart campus: A system and a study,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. ieeexplore.ieee.org, pp. 94–99.

Rahimi, H., Nur Zincir-Heywood, A. and Gadher, B. (2013) “Indoor geo-fencing and access control for wireless networks,” in *2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)*. ieeexplore.ieee.org, pp. 1–8.

Raza, S. *et al.* (2017) “Building the Internet of Things with bluetooth smart,” *Ad Hoc Networks*. Elsevier, 57, pp. 19–31.

Slack, F. and Rowley, J. (2002) “Kiosks 21: a new role for information kiosks?,” *International journal of information management*. Elsevier. Available at: https://www.sciencedirect.com/science/article/pii/S026840120100041X.

Talei, H. *et al.* (2015) “Smart campus microgrid: Advantages and the main architectural components,” in *2015 3rd International Renewable and Sustainable Energy Conference (IRSEC)*. ieeexplore.ieee.org, pp. 1–7.

Terán, M. *et al.* (2017) “IoT-based system for indoor location using bluetooth low energy,” in *2017 IEEE Colombian Conference on Communications and Computing (COLCOM)*. ieeexplore.ieee.org, pp. 1–6.

Vafin, A. (2017) “Negotiation with Dominant Supplier: Power Determination, Partnership, and Joint Buying,” *International Journal of Contemporary Financial Issues*. hcommons.org. Available at: https://hcommons.org/deposits/item/hc:44887/.

Vafin, A. (2018) “Volume Discount Sensitivity Analysis for Optimal Pricing Strategies in B2B Firms,” *Empirical Quests for Management Essences*. researchberg.com. Available at: https://researchberg.com/index.php/eqme/article/view/33.

Xavier, L. A. (2019) “Identification of Age Voiceprint Using Machine Learning Algorithms,” *ResearchBerg Review of Science and Technology* . researchberg.com, 1(1), pp. 1–16.

Yin, C. *et al.* (2015) “A literature survey on smart cities,” *Science China. Information Sciences*. Springer, 58(10), pp. 1–18.

Zhuang, Y. *et al.* (2016) “Smartphone-Based Indoor Localization with Bluetooth Low Energy Beacons,” *Sensors* . mdpi.com, 16(5). doi: 10.3390/s16050596.

Zhuhadar, L. *et al.* (2017) “The next wave of innovation—Review of smart cities intelligent operation systems,” *Computers in human behavior*. Elsevier, 66, pp. 273–281.