



A Framework of Universities' Smart Campus to Detect and Mitigate Vulnerabilities for IoT Devices

Mazlina Abdul Majid

Universiti Malaysia Pahang, Malaysia, mazlina@ump.edu.my  <https://orcid.org/0000-0001-9068-7368>


Husnul Ajra

Universiti Malaysia Pahang, Malaysia, husnul5606ice@gmail.com  <https://orcid.org/0000-0002-9663-9444>


Ali Shehadeh

Yarmouk University, Jordan, ali.shehadeh@yu.edu.jo  <https://orcid.org/0000-0002-6875-4824>

Md. Shohidul Islam

Universiti Malaysia Pahang, Malaysia, msi.ice.ru@gmail.com  <https://orcid.org/0000-0002-0786-5221>

Khalid Adam Ismail Hammad

Universiti Malaysia Pahang, Malaysia, khalidadam@ump.edu.my  <https://orcid.org/0000-0001-6232-7154>

Abstract: One of the most persuasive technologies in developing universities' smart campus applications is the Internet of Things (IoT) technique. Deploying thousands of readily available devices connected to IoT systems by ignoring device vulnerabilities and threat strategies in smart campus infrastructure is exacerbating security challenges. Moreover, unreliable sensing, transmission, or processing of IoT devices, false observations, long delays, and data reports reveal the vulnerability of efficient smart campus infrastructure. Some transient errors or attacks also occur here due to many vulnerable device memory, processing power, soft errors, and battery imperfections. The need to overcome significant challenges, including advanced training-rich IoT devices, credible designers, reliability, scalability, interoperability, availability, and performance, has motivated our aim to implement intelligent platforms for university campuses. In this study, we propose an operational framework for smart campuses to detect and mitigate vulnerabilities aimed at processing a comprehensive security certification of IoT devices, including introducing a smart model for university campuses. We discuss challenges, detection, and mitigation of vulnerabilities associated with smart campuses. From the literature exploration, we found that machine learning and DNN are capable of being used to detect malicious behaviour and vulnerable sources. Thus, the proposed framework is expected to provide better security and be capable of meeting the compliance of existing university services.

Keywords: Device, IoT, Smart Campus, University, Vulnerability

Introduction



Currently, there are various challenges in education and educational institutions across the world, including student competitiveness, competency, institution building, education delivery infrastructure, improving teacher skills, relational infrastructure, digital technology enthusiasm, and so on. From this context, the concept of creating a smart model for university campuses has emerged. IoT technology is one of the dominant technological skills in the smart university campus (Jabbar et al. 2021), (Ahmed and Majid 2019) which has risen vigorously in popularity commencement in 2016. An adopted IoT platform can drive efficient resource utilization and enable the evolution of academic campuses. All the interconnected intelligent equipment (things) of this platform help construct smart universities, which promise sustainable development and transition to green campuses. Many educational institutions in several countries around the world have started building smart campuses. These include several universities in Malaysia, Vietnam, and Singapore that have allocated a large portion of their budgets to education with the aim of creating smart campuses.

However, to contact thousands or lots of pieces of equipment projected to make up the IoT on academy campuses, developers will have to overpower consequential undertaking challenges, including security, trust, scalability, reliability, availability, interoperability, mobility, and performance. Among these challenges, reliability (Azghiou et al. 2020) has been determined as the first of the required matters for well-organized IoT. Inconsistent transmission, body perceiving, and processing due to insufficient reliability can generate inaccurate monitoring reports, lose data, and cause long delays, leading to vulnerabilities across intelligent university campus applications. The more harmful behavior of the untrustworthy smart campuses (Anagnostopoulos et al. 2021), for instance, transient imperfections that emerge in IoT appliances (also apprehended as soft errors), unlike design or manufacturing flaws, do not happen coherently. Rather, all intermittent errors are generated by outward circumstances to smart IoT applications, such as energized particles hitting the chips. These affairs do not provoke endless outward impairment to the IoT devices but can adjust accumulated values or signal transfers and consequently induce faulty smart campus application implementation.

Although several studies have analyzed and evaluated the reliability of IoT, various approaches have been suggested to mitigate the arising soft errors in IoT founded on software (Alsariera, Majid, and Zamli 2015b) determinations and hardware. For norm, the IoT's reliability problem from the matter of the idea of the transcendent strategy of reliability appraisal utilizing MIL-HDBK 217 has discoursed. With the suitable process of reliability (Nagowah, Ben Sta, and Gobin-Rahimbux 2020) evaluation operating MIL-HDBK 217, only the reliability of hardware can be evaluated, whereas the circumstances in IoT are more complex because thousands or millions of individual devices (things), human users, and software programs (Majid, Zain, and A. Hermawan n.d.) are engaged in the network. System reliability in IoT components (things) is a concern not only for data failure rates in smart campuses but also for human factors and software, which makes implementing IoT in smart campus-sensitive applications challenging.

Although several studies have been carried out before, this problem is still insufficiently explored, prompting attention to research gaps, and a new approach is therefore needed. Therefore, the objective of this study is to construct an operational framework capable of mitigating IoT (device) error vulnerability, maintaining

reliability, and evaluating the performance of smart campuses. Likewise, to maintain the safe reliability of urban big data and security in its transactions, this study introduces a desired smart campus model for university campuses. model using the access network principle of IoT to build a smart city. The contributions of this paper are as follows:

- This work will cooperate with developing and researching a smart campus framework.
- We introduce an operational framework and present its process.
- This paper proposes a reliability-enabled smart campus model by mitigating the vulnerability of IoT devices.

The residue of this study is arranged as follows. In Section II, this study presents the problem exploration and arising research question. Then Section III introduces the literature review based on smart campus. In Section IV, this study demonstrates the methodology with an operational framework according to the review. Section V presents a research discussion based on the proposed smart campus model. Finally, Section VI concludes this study.

Problem statement and research questions

Problem Statement

Smart campus implementation is incorporated using the things internet. IoT is a network that interconnected intelligent appliances supplying rich information, but it can also be a safety nightmare as it mostly has issues with reliability and quality (Imbar, Supangkat, and Langi 2020). The current IoT devices are the retail type, not including specified reliability and no failure rate data, such as the mean time to failure (MTTF) or mean time between failures (MTBF). The reliability of IoT networks is the primary concern in IT today as vulnerabilities on the devices could resulting various fault responses, including incorrect decision-making that potentially be life-threatening for end-users on campus (Adam, Mohamed, and Ibrahim 2021), (Ibrahim et al. 2020), (Ardiansyah, Majid, and Zain 2017), (Sultan Mahmud, Islam, and Rahman 2017).

Reliability for electronic devices has been estimated mostly using reliability prediction standards called MIL-HDBK-217. In 1961, the first version of MIL-HDBK-217 was designed and had not been updated since 1995. Despite its constraints, MIL-HDBK-217 is yet utilized by more than 80% of manufacturers for assessing trustworthiness. There are different commercial and industrial standards for computing reliability on electronic devices, such as RIAC's 217PlusTM methodology and tool. RIAC's 217PlusTM is more complex in calculating reliability compared to MIL-HDBK-217 standards. To overcome the limitation of the existing hardware reliability standard, IEEE constructed a standard named IEEE Std.1413 in 2009 (Masitry et al. 2013), (Alsariera, Majid, and Zamli 2015a) based on the standard model for hardware reliability prediction. Reliability for IT components is not only calculated from the viewpoint of hardware but also software.

There are existing standards for software reliability, such as ISO/IEC 25000 (software and data quality) and IEEE 1633-2016 (IEEE instructed approach on software reliability). Standards for reliability prediction for IoT devices are available both for hardware and software, but such prediction is mainly conducted for single checking without considering the ecosystem of IoT as a whole in one place, such as a smart campus. The

ecosystem of IoT covers hardware, software, network, personnel, and physical and organizational ingredients. Increasing the reliability, detection, and mitigation of the vulnerabilities of IoT devices is significant from the viewpoint of the IoT ecosystem. In order to focus on research issues and gaps, the vulnerabilities of IoT devices in the smart campus scheme are presented in Figure 1 IoT authentication designs typically secure smart applications by building reliability into connected IoT devices and their designs. Unauthorized IoT devices and the inadequacy of their design pose a major challenge in maintaining authentication in building smart campuses.

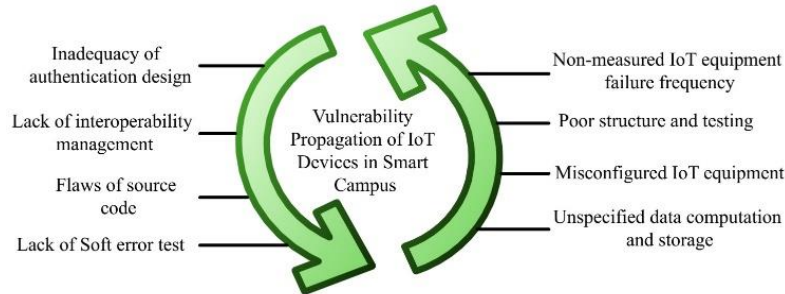


Figure 1. Propagation of IoT Device Vulnerabilities in Smart Campus

IoT interoperability can emerge as a major concern in smart campus applications. Overlapping or non-standard connectivity in IoT devices and their systems creates a lack of interoperability, which is a major obstacle to achieving reliability in smart applications. The risk that source code flaws pose in connected networks of IoT devices undermines the reliability of smart academy infrastructure. Achieving the expertise available in IoT devices to remove source code flaws can be a significant concern. Further, how well IoT's resource-constrained devices, internal and external networks, and software are working depends on soft error (transient in nature) test parameters to achieve the objectives and reliability of smart applications. Smart campus applications involve all types of data collection, computation, processing, and storage through all types of IoT devices. In this regard, the unspecified large amount of data computation and storage can be another constraint in IoT-enabled smart campuses.

However, the failure frequency rate in non-metered IoT equipment settings determines the evaluation of all parameters, such as network performance, stability, and reliability. The strategies of non-measured IoT equipment failure frequency mitigation are key challenges in achieving reliability in smart campus applications. Poor infrastructure and testing of IoT equipment can hinder the functioning of a proper smart campus. Consequently, fundamental security and reliability issues are faced with challenges regarding smart campus services for users. Achieving good system security and reliability requires identifying thousands of device configuration vulnerabilities and irrelevant issues. Mismanagement and misconfiguration of IoT devices will weaken the security and reliability functions, which will lead to the collapse of the smart campus access network system. Thus, this study aims to improve reliability by proposing a framework to detect and mitigate the vulnerabilities of IoT devices from the smart university campus.

Research Questions

- What are the implications of vulnerabilities of IoT devices in smart campuses from the reliability concern perspective?

- What are the parameters that contribute to the vulnerabilities of IoT devices for smart campus infrastructure in terms of reliability concerns?
- How to mitigate the vulnerabilities of IoT equipment to ensure reliability in smart campuses?

Literature Review

Smart Campus and IoT

The rapid development of IoT is leading universities to become smart campuses. Executing IoT operates to skillful resource use and fosters the evolution of academy campuses, where connected intelligent things (devices) are supporting to make the smart campus, which promises to acquire sustainable development and change into green campuses (Elerath and Pecht 2012), (Min-Allah and Alrashed 2020). Thus, this segment supplies an overview of the smart campus implemented IoT, the demeanor of the IoT reliability, and techniques being used to efficiently mitigate the faults. Due to the mission-critical or safety-critical character of IoT schemes, the IoT devices must conduct reliably during the determined mission period. In addition, reliability is an important requirement for IoT adoption in intelligent applications (Zaballos et al. 2020), (Pokorni 2019). Failures in assisting IoT appliances, transient faults (soft errors), failures to grab vital data, data corruption, any network outage, or failure during broadcast or repository may generate destructive impacts, for instance, economic loss, mission failure, and disservices to environments and people (Adam et al. 2021), (Majid 2022). Thus, reliability analysis and design are necessary for researchers, developers, and even consumers prior to IoT can be extensively employed on academy campuses.

Existing Prediction Standard/ Method

Several studies have been proposed on IoT's fault tolerance to overcome the reliability problem. Earlier research papers have utilized MIL-HDBK 217 as a standard method for reliability appraisal (Adam et al. 2021). However, the reliability of IoT is not merely a matter of the IoT failure rate but also of human and software aspects in smart universities. Various studies aim for sustainable development and/or smart campus to support teaching activities, water, transportation, energy, and other resources (Chagnon-Lessard et al. 2021), (Valks et al. 2020). In (Nguyen, Le, and Dao 2021), it introduces an IoT-enabled university campus platform for people and environmental flow observation. In (Fortes et al. 2019), a comprehensive work was demonstrated, where a smart campus named SmartUMA is implemented by the University of Málaga and aims at smart parking, intelligent space, and smart education utilizing the IoT to operate it. Hence, a mobile application of SmartUMA named UMA allows students to boldly access learning materials while watching videos and doing distance learning activities that are developed by teachers. However, the issue of reliability was not taken into consideration while developing the UMA Smart Campus framework to conduct education programs using IoT on this platform.

Khajenasiri et al. (Khajenasiri et al. 2017) executed an observation on the IoT solutions for intelligent energy management to amenities smart city applications. They have remarked that, at current, IoT has been deployed in significantly few application dimensions to benefit people and technology. The scope of IoT is quite vast, and in

the nearest future, IoT will be capable of capturing nearly all application sites. They referred that energy conservation is one of the critical parts of the community, and IoT can assist in designing an intelligent energy management scheme that will preserve both money and energy. They represented an IoT structure regarding the smart city thoughts. The authors also explained that one of the demanding works in acquiring this is the imperfection of IoT software and hardware. They instructed that the issues must be settled to provide an efficient, reliable, and user favorable IoT design.

Another concerning aspect regarding contrivance trustworthiness in IoT is the inclination for existing sensing devices to 'fail dirty' (Rico-bautista and Medina-c n.d.). This phenomenon involves a strategy where a sensor persists in sending inaccurate readings afterward, having suffered the deficiency. It is a prominent, still little-apprehended issue that is infectious in IoT domains. Mainly this point is challenging to analyze since the sensing devices emerge to be usually performing.

Table 1. The Summary of Findings from Related Literature

Ref.	Focus study	Key contributions	Similar findings in review studies	Additional findings in review studies
(Rico-bautista and Medina-c n.d.)	Explicated the emerging technological concepts of smart university with IoT	Presented the development of conceptual success frameworks concerning problem circumstances, motives, and features of smart universities based on scientific publications.	Overview of smart campus with IoT from the technical perspective	- Detail of ideas, technologies, and architectures of smart universities - Express socio-technological and educational paradigms in IoT evolution - Basic components and the "smartification" process of a university.
(Wigati n.d.)	Conducted Systematic Literature Review (SLR) on the impact of smart campus implementation	Offering a virtual smart campus with literature review approaches and techniques to make student interest and enthusiasm in higher education.	Synopsis of the smart campus	- Explicit the smart campus impact and qualities on higher education - Represent the enabling technologies and evaluations of smart campus
(Malatji 2017)	Motives to focus on the smart transitions and shortcomings in the context of African universities.	As case studies, it emphasized the development and implications for becoming a smart campus from the perspective of African universities.	Synopsis of smart campus development	- A detailed discussion of the structural model with the identification of features and key performance indicators for a smart campus. - Expressed smart initiatives based on the case study for South African universities.

(Anagnostopoulos et al. 2021)	Choose the socially acceptable surveillance approach in IoT-enabled smart campuses.	Provides a comparative assessment of selected systems and their resulting outcomes on existing smart campuses in terms of surveillance systems.	Synopsis of the smart campus with IoT core empowering technologies	<ul style="list-style-type: none"> - Details of the surveillance systems and conceptual infrastructures for IoT-enabled intelligent campus. - Comparative valuation in the dimensions of surveillance procedures for smart campus - Solution method of surveillance schemes in the smart campus
(Imbar et al. 2020)	Conducted the literature review on indicator dimensions of the smart campus environment	Providing a review of terminology and structure of the intelligent campus so that stakeholders can accumulate better understanding and knowledge.	Overview of the smart campus terminology	<ul style="list-style-type: none"> - Detailing a paradigm alteration from outmoded to smart campus, including terminology and framework - Exposition of interactive iCampus design and UMA Smart Campus in terms of relevant areas
(Ujang et al. n.d.)	Aims to focus on the future vision and cover all components of the smart campus.	Elucidates a framework for how IoT can be employed on an innovative university campus to manipulate daily educational activities and welcome novel visions.	Recap of the smart campus with sustainability	<ul style="list-style-type: none"> - Description of the concept of the smart city and smart university with elements. - Exposition of E-JUST as a smart campus model. - Benefits and challenges of sustainable smart campuses

The impact of a misreading transmitted in an IoT scheme can be essential when we consider that functionality generally has a physical impact on people's lives (Rico-bautista and Medina-c n.d.). Table 1 shows the summary of the associated literature on the smart campus. The studies cited in the table provided the impetus for the review process of this work. However, these studies did not consider the reliability, dependability, or soft errors of constructing smart campuses. The issues of Identifying the vulnerabilities of IoT devices and determining the failure rate of IoT in smart campuses are not clarified. Furthermore, some transient malfunctions of IoT devices, unreliable sensing processing, false data reports, battery imperfections, and long delays expose the vulnerabilities of efficient smart campus infrastructure. Therefore, the goal of this study is to construct an operational framework capable of mitigating IoT devices' error vulnerability, maintaining reliability, and evaluating the performance of smart campuses.

Gap Analysis

Typically, standards or approaches for reliability prediction for IoT appliances are unrestricted for all types of software and hardware. But such prediction is primarily accomplished for single checking without assessing the ecosystem of IoT as an entirety in one area, like as a smart campus. The ecosystem for the IoT domain covers hardware, software, network, personnel, physical, and organization, where these can face vulnerabilities. In these smart sectors, the improvement of detection and mitigation of the vulnerabilities of IoT devices is significant from the perspective of the IoT environment using reliability analysis.

Research Objectives

The study aims to develop a framework that is able to mitigate the vulnerabilities' fault in the IoT (devices), maintain the reliability in the smart campus that operate under fault effects on an IoT, and evaluate the framework performance. The following objectives have been formulated to achieve these objectives of the university smart campus framework.

- Identifying the appropriate parameters that contribute to the vulnerabilities of IoT devices in smart campuses.
- Developing a framework that is capable of detecting and mitigating the vulnerabilities' faults in the smart campus.
- Evaluation metrics will be used to design the framework in terms of reliability.

Methodology

Operational Framework

The Smart applications interrelated with IoT systems require the modernization of existing systems to make them more dynamic and efficient. Moreover, existing smart applications reveal some vulnerabilities of IoT devices, such as transient faults, unreliable sensing, imperfections, and long delays that need to be identified and mitigated. In accordance, this study illustrates a well-defined methodological research operational framework through Figure 2 for detecting and mitigating fault vulnerabilities in the smart campus setting. This scheme consists of a literature review, fault injection, identifying the most vulnerable part of the smart campus, developing a framework to reduce the faults, evaluating the most vulnerable part's reliability, and analyzing the result. Each phase in this methodical process will be partitioned into various steps that can be attained in an appropriate time frame.

In the first phase, the study sets a plan before implementing the work to determine all aspects of the research. The central sub-component in this phase is collecting and analyzing the literature review from the works of smart campuses, which is regarded as one of the maximum vital phases of the research framework. In this fact, the study determines the limitations of existing studies and defines the problem statement of the research. Moreover, the objectives, significance, and scopes of the study will also be determined in this component. In this context, identifying fault injection and formatting methods needed that will be used to measure the proposed framework.

In the second phase, this study comprises data collection, case study selection, main interview, faults injection, and reliability analysis. This phase answers the research questions, namely, what are the implications of vulnerabilities of IoT devices in smart campuses? How can it be confirmed that decision is engaged by the IoT devices based on vigorous data, specifying the challenges at lower layers of IoT device vulnerabilities? How to mitigate the vulnerabilities of IoT devices on the smart campus model? This phase involves faults injection and case study.

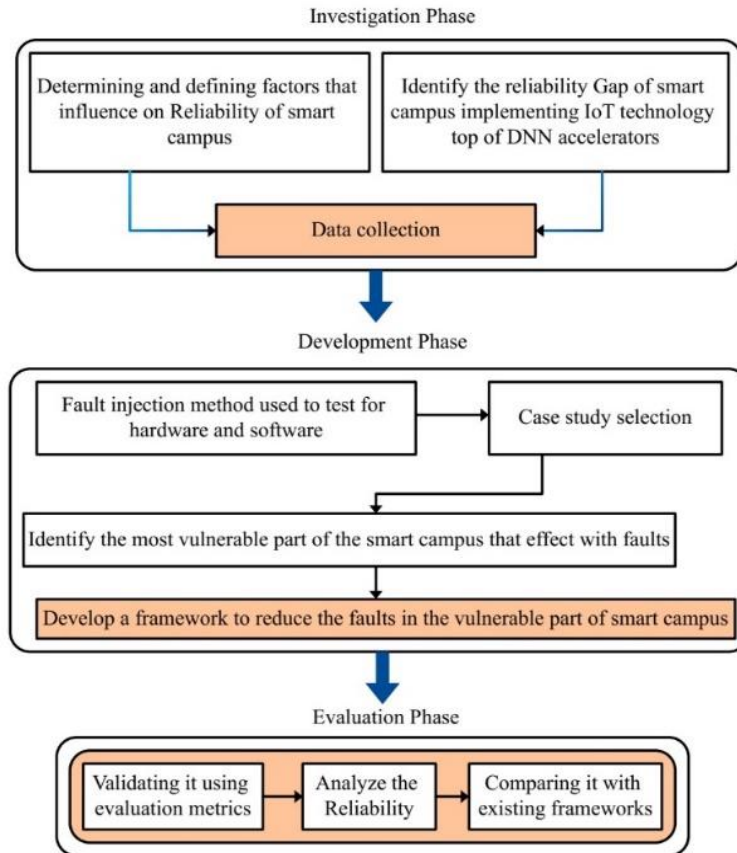


Figure 2. Proposed operational framework

In the third phase, it is incorporated the development of the framework. The framework will develop to evaluate and reduce the faults and vulnerabilities that occur due to the IoT elements (things), software, and human factors. To accomplish the third objective, we will measure two factors: (1) Architectural Vulnerability Factor (AVF) that makes the possibility that a solo fault on IoT devices (things) will consequence in error. It is employed to explore how smart campus applications respond to errors in IoT devices. (2) Program Vulnerability Factor (PVF), which is the possibility that a solo fault modifies the decision-making and propagates to other smart campus applications. Therefore, to assess the stability of the smart campuses, we accomplish described model sensitivity studies from various views by assessing three evaluation metrics as follows; IoT devices (things) vulnerability analysis, software vulnerability analysis, and human vulnerability analysis to identify the vulnerability parts of the smart campus. Next, the framework to reduce the faults in the vulnerable most vulnerable parts of the smart campus, which reduces the fault, thus enhancing the reliability of the smart campus applications.

In this final phase, we evaluate the proposed framework, based on the previous result, in typical smart applications of the smart campus, online survey data by validating the reliability based on a set of follow-up questionnaire questions. This research is in the domain of smart campuses, which is in its early stages and has a profound theoretical background. Also, the nature of this research is exploratory. The data for this survey will be based on a minimum of 100 or more respondents from institutions of higher learning based in Malaysia, such as mainly the education sector and industrial IoT applications or IoT companies. The survey instrument will be prepared by considering the exploratory nature of the study.

IoT-enabled Smart Campus Model

This section discusses the relevant tasks of smart city construction as a proposal. Figure 3 shows smart campus model that introduces intelligent urban policies. This model will employ sensors, actuators, network devices, and so on. It can enable surveillance systems for monitoring purposes. For information communication, this scheme will work using the access network and store it in cloud storage. Besides, reliability prediction standards or methods for IoT devices in a smart campus can be applied to this model. This system will detect and mitigate the vulnerabilities using the mitigation technique and DNN approach. According to the operations of the operational framework mentioned in the previous section, this smart campus model will i) apply AVF for exploring the responses from IoT device errors, ii) embed PVF for decision-making based on explored responses in terms of errors, iii) employ evaluation metrics for vulnerabilities analysis and detection, and iv) mitigate vulnerabilities for enhancing the reliability. This model will involve detection and mitigation methods to assess and mitigate errors and vulnerabilities caused by IoT elements (things) such as hardware, software, and human factors. The campus users such as staff, students, teachers, or officers can obtain quality services.

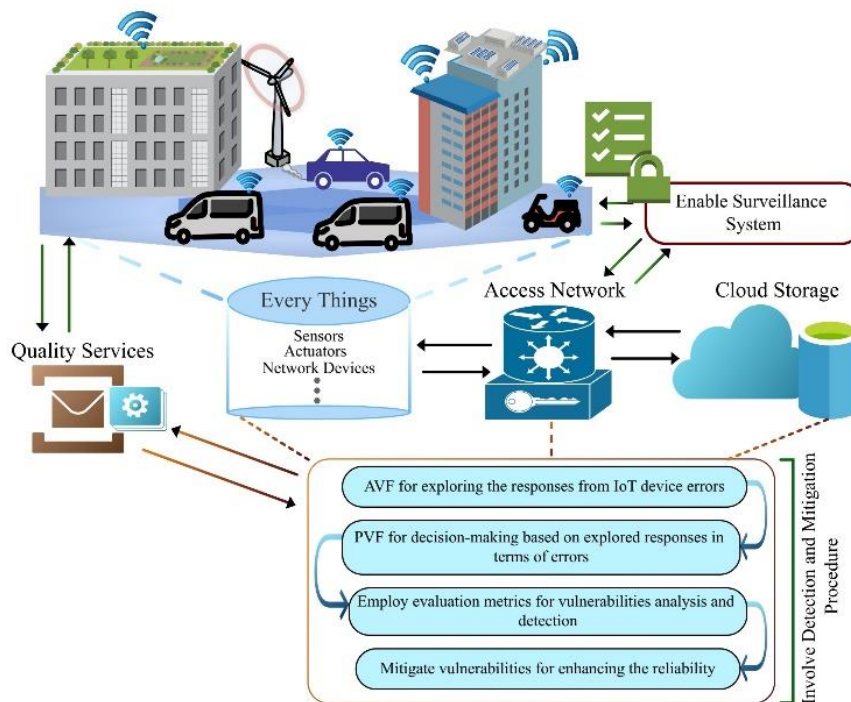


Figure 3. Smart campus model

We have only presented this model in this paper, and our next task is to improve and implement it. Furthermore, intending to build smart cities can reform a critical role in maintaining the secure reliability of big urban data

and its transaction security, including monitoring. In this consideration, this smart campus design will ensure service availability and mobility to participants by eliminating data reports, long delays, inefficiencies, processing errors, and infrastructure vulnerabilities from the perspective of intelligent university services.

Conclusion

For an educational institution or university to come under smart campus, all the indicators of smart structure should be addressed. Implementing smart campus applications by providing knowledge study criteria and intelligent services is essential to enhance the quality of the university's learning environment. It has been focused on building a smart campus for practical and acceptable management of universities. Emphasis is placed on studying and formulating appropriate motivational methods to identify the most vulnerable parts of IoT-enabled smart campus devices. In this case, we have proffered the operational structure of a smart campus and an intelligent campus model by looking at all the indicators to bring an educational institution or university under an intelligent campus. Adequate procedures have been presented to overcome the real impact of unknown vulnerabilities, errors and security situations in advanced educational institutions. The well-defined methodological research mentioned in the paper should take into account the operational framework where the assessment and analysis of vulnerable IoT devices related to smart campus deployments and reliable IoT devices are essential. Our future work is to improve IoT-enabled smart campus infrastructure for a safe education system by assessing device vulnerabilities and improving its quality based on follow-up and survey data.

Acknowledgements or Notes

This study has been funded by Green Technology Research Lab, Universiti Malaysia Pahang (UMP) under the Malaysia National Research Grant FRGS/1/2018/ICT04/UMP/02/4, and UMP Research Grant (RDU190167 and PGRS220338). This study is conducted in collaboration with Yarmouk University, Jordon, and supported by Bangabandhu Sheikh Mujibur Rahman Science & Technology University, Bangladesh.

References

- Adam, Khalid, Izzeldin Ibrahim Mohamed, and Younis Ibrahim. 2021. "A Selective Mitigation Technique of Soft Errors for DNN Models Used in Healthcare Applications: DenseNet201 Case Study." *IEEE Access* 9:65803–23. doi: 10.1109/ACCESS.2021.3076716.
- Ahmed, Firas D., and Mazlina Abdul Majid. 2019. "Journal of Network and Computer Applications Towards Agent-Based Petri Net Decision Making Modelling for Cloud Service Composition : A Literature Survey." *Journal of Network and Computer Applications* 130(December 2018):14–38. doi: 10.1016/j.jnca.2018.12.001.
- Alsariera, Y. A., M. A. Majid, and K. Z. Zamli. 2015a. "A Bat-Inspired Strategy for Pairwise Testing." *ARN Journal of Engineering and Applied Sciences* 10(18):8500–8506.
- Alsariera, Y. A., M. A. Majid, and K. Z. Zamli. 2015b. "SPLBA: An Interaction Strategy for Testing Software

- Product Lines Using the Bat-Inspired Algorithm.” Pp. 148–53 in *In 2015 4th International Conference on Software Engineering and Computer Systems (ICSECS), IEEE*.
- Anagnostopoulos, Theodoros, Panos Kostakos, Arkady Zaslavsky, Ioanna Kantzavelou, Nikos Tsotsolas, Ioannis Salmon, Jeremy Morley, and Robert Harle. 2021. “Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A Survey.” *IEEE Access* 9:131926–54. doi: 10.1109/ACCESS.2021.3114447.
- Ardiansyah, Soleh, Mazlina Abdul Majid, and Jasni Mohamad Zain. 2017. “Knowledge of Extraction from Trained Neural Network by Using Decision Tree.” *Proceeding - 2016 2nd International Conference on Science in Information Technology, ICSITech 2016: Information Science for Green Society and Environment* 220–25. doi: 10.1109/ICSITech.2016.7852637.
- Azghiou, Kamal, Manal El Mouhib, Mohammed Amine Koulali, and Abdelhamid Benali. 2020. “An End-to-End Reliability Framework of the Internet of Things.” *Sensors (Switzerland)* 20(9):1–23. doi: 10.3390/s20092439.
- Chagnon-Lessard, Noemie, Louis Gosselin, Simon Barnabe, Tunde Bello-Ochende, Sebastian Fendt, Sebastian Goers, Luiz Carlos Pereira Da Silva, Benedikt Schweiger, Richard Simmons, Annelies Vandersickel, and Peng Zhang. 2021. “Smart Campuses: Extensive Review of the Last Decade of Research and Current Challenges.” *IEEE Access* 9:124200–234. doi: 10.1109/ACCESS.2021.3109516.
- Elerath, Jon G., and Michael Pecht. 2012. “IEEE 1413: A Standard for Reliability Predictions.” *IEEE Transactions on Reliability* 61(1):125–29. doi: 10.1109/TR.2011.2172030.
- Fortes, Sergio, José Antonio Santoyo-Ramón, David Palacios, Eduardo Baena, Rocío Mora-García, Miguel Medina, Patricia Mora, and Raquel Barco. 2019. “The Campus as a Smart City: University of Málaga Environmental, Learning, and Research Approaches.” *Sensors (Switzerland)* 19(6). doi: 10.3390/s19061349.
- Ibrahim, Younis, Haibin Wang, Man Bai, Zhi Liu, Jianan Wang, Zhiming Yang, and Zhengming Chen. 2020. “Soft Error Resilience of Deep Residual Networks for Object Recognition.” *IEEE Access* 8:19490–503. doi: 10.1109/ACCESS.2020.2968129.
- Imbar, Radiant Victor, Suhono Harso Supangkat, and Armein Z. R. Langi. 2020. “Smart Campus Model: A Literature Review.” *7th International Conference on ICT for Smart Society: AIoT for Smart Society, ICISS 2020 - Proceeding*. doi: 10.1109/ICISS50791.2020.9307570.
- Jabbar, Waheb A., Chong Wen Wei, Nur Atiqah Ainaa M. Azmi, and Nur Aiman Haironnazli. 2021. “An IoT Raspberry Pi-Based Parking Management System for Smart Campus[Formula Presented].” *Internet of Things (Netherlands)* 14:100387. doi: 10.1016/j.iot.2021.100387.
- Khajenasiri, Iman, Abouzar Estebarsari, Marian Verhelst, and Georges Gielen. 2017. “A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications.” *Energy Procedia* 111(September 2016):770–79. doi: 10.1016/j.egypro.2017.03.239.
- Majid, M. B. A., J. B. M. Zain, and A. Hermawan. n.d. “Recognition of Malaysian Sign Language Using Skeleton Data with Neural Network.” Pp. 231–36 in *In 2015 International Conference on Science in Information Technology (ICSITech), IEEE*.
- Majid, Mazlina Abdul. 2022. “Big Data Prediction Framework for Weather Temperature Based on MapReduce Algorithm.” 13–17.

- Malatji, Esrom Mahlatsi. 2017. "The Development of a Smart Campus - African Universities Point of View."
- Masitry, Ananthi Krishnasami, Mazlina Abdul Majid, M. Zulfahmi Toh, Universitas Ahmad Dahlan, and Jln Prof Soepomo. 2013. "An Investigation on Learning Performance among Disabled People Using Educational Multimedia Software : A Case Study for Deaf People Department of Mathematics Education." 5(6):9–20.
- Min-Allah, Nasro, and Saleh Alrashed. 2020. "Smart Campus—A Sketch." *Sustainable Cities and Society* 59(December 2019):102231. doi: 10.1016/j.scs.2020.102231.
- Nagowah, Soulakshmee D., Hatem Ben Sta, and Baby Gobin-Rahimbux. 2020. "A Systematic Literature Review on Semantic Models for IoT-Enabled Smart Campus." *Applied Ontology* 16(1):27–53. doi: 10.3233/ao-200240.
- Nguyen, Son Thanh, Bich Ngoc Le, and Quy Xuan Dao. 2021. "AI and IoT-Powered Smart University Campus: Design of Autonomous Waste Management." *Proceedings - 2021 International Symposium on Electrical and Electronics Engineering, ISEE 2021* 139–44. doi: 10.1109/ISEE51682.2021.9418672.
- Pokorni, Slavko. 2019. "Reliability and Availability of the Internet of Things." *Vojnotehnicki Glasnik* 67(3):588–600. doi: 10.5937/vojtehg67-21363.
- Rico-bautista, Dewar, and Yurley Medina-c. n.d. "Smart University : A Review from the Educational and Technological View of Internet of Things." 1:427–40. doi: 10.1007/978-3-030-11890-7.
- Sultan Mahmud, Mohammad, Md Shohidul Islam, and Md Ashiqur Rahman. 2017. "Smart Fire Detection System with Early Notifications Using Machine Learning." *International Journal of Computational Intelligence and Applications* 16(2). doi: 10.1142/S1469026817500092.
- Ujang, Norsidah, Tomohiro Fukuda, Anna Laura Pisello, and Dinko Vukadinovi. n.d. *Resilient and Responsible Smart Cities*. Vol. 1.
- Valks, Bart, Monique H. Arkesteijn, Alexander Koutamanis, and Alexandra C. den Heijer. 2020. "Towards a Smart Campus: Supporting Campus Decisions with Internet of Things Applications." *Building Research and Information* 1–20. doi: 10.1080/09613218.2020.1784702.
- Wigati, Nurma Ayu. n.d. "Smart Campus Implementation Effects towards Student Interest in Higher Education : A Systematic Literature Review." 101–6.
- Zaballos, Agustín, Alan Briones, Alba Massa, Pol Centelles, and Víctor Caballero. 2020. "A Smart Campus' Digital Twin for Sustainable Comfort Monitoring." *Sustainability (Switzerland)* 12(21):1–33. doi: 10.3390/su12219196.