A Novel IoT Architecture for Seamless IoT Integration into University Systems

Wafa Altwoyan, Ibrahim S. Alsukayti
Department of Computer Science, College of Computer, Qassim University
Buraydah, Saudi Arabia

***Abstract*—IoT architectures play critical roles in guiding IoT system construction and enhancing IoT integration. However, there is still no standardized IoT architecture that meets the varying requirements of different IoT deployments. Although this has been a focus within the research community, no specific attention has been paid to optimizing an IoT architecture toward seamless IoT integration in educational environments. Moreover, different advanced system aspects have not been considered for designing an optimized IoT architecture. These include the need for complete security and privacy support, a highly responsive system, dynamic interactivity, and wide-range IoT connectivity. Such considerations are important considering the complexity and multidimensionality of integrating IoT in educational environments. In this paper, we introduced a novel IoT architecture with the main objective of facilitating the effective integration of IoT into university systems. It also aims at optimizing the IoT-integrated system with advanced aspects to enhance system security, responsiveness, and IoT connectivity. The proposed architecture provides a modular and scalable design of six architectural layers in addition to a vertical layer that provides security support across the architecture. Only the most relevant and critical layers are added to the architecture to maintain a practical trade-off between effective modularity and less complexity. Compared with other IoT architectures, the proposed one ensures high reliability, data management, full security support, responsiveness, and wide coverage while maintaining acceptable complexity.**

Keywords—Internet of things; architecture; smart campus; education

I. Introduction

Advancements in Information and Communication Technology (ICT) have recently enabled the effective transformation of conventional educational systems to a more efficient and sustainable level. The high dependency on technology and digital services allows substantial investment of recent technologies in enhancing traditional educational methods. The ICT revolution leads traditional learning to be moved to new paradigms such as e-learning and distance learning. This creates opportunities for further improvements regarding the educational activities and processes. Such technological advancements in the education domain can be even more optimized with the best leverage of recent technologies. One of these is the Internet of Things (IoT) technology which is projected to change several facets of the educational environment [1].

IoT provides a technological revolution that enables effective interaction between people, processes, data, and things. It facilitates the effective provisioning of smart services in different domains including healthcare [2], industry [3], and agriculture [4]. In addition, learning is one of the most perceptible human actions affected by IoT, turning the educational process into a revolutionary system in the near future. IoT enables educational environments to be significantly extended by combining physical and digital objects. IoT finds its way into education to provide advanced support in enhancing many aspects. These include streamlining educational processes, making the most use of data, and improving sustainability. IoT can serve as a catalyst for improving the current knowledge-transfer model to be more interactive and collaborative. The teaching-learning process would be actively engaging with the efficient use of IoT in education systems [5].

However, integrating IoT in educational environments is still a challenging process. Careful consideration of the complexity and multidimensionality of such environments is important before going any further through this process. At the fundamental level, architectural planning is the key to optimizing IoT integration in educational environments. The importance of developing IoT architecture lies in its critical role in guiding system construction and facilitating IoT integration. Such a challenging IoT integration can be fundamentally simplified by developing an efficient IoT architecture. Despite the wide adoption of IoT technology in different domains, there is still no standardized IoT architecture that meets the varying requirements of different IoT deployments [6]. Several design approaches have been introduced for the development of an effective IoT architecture. They vary in granularity and the number of architectural layers in addition to considering different system aspects.

However, fundamentally addressing the efficiency and complexity of integrating IoT into the specific environments of educational institutions has not been considered yet. The focus has been only on addressing the main IoT system aspects, particularly data collection, transmission, processing, and application. No particular attention has been devoted to the specific characteristics of educational environments when integrated with IoT. These include the need for complete security and privacy support, highly responsive system, dynamic interactivity, and wide-range IoT-specific connectivity. Still there is a compelling need for effective design of an IoT architecture to facilitate IoT integration and accelerate IoT adoption in these dynamic environments. This paper aims at addressing such a need by establishing an IoT architecture while taking into account advanced technological considerations. These include edge computing, IoT accessibility, cloud computing, and full security integration.

The following section, Section II, of this paper presents the related work. In Section III, an overview of the integration of IoT in education environments is provided. Section IV introduces the proposed IoT architecture. Then, a simple use case demonstrating the implementation of the proposed architecture is presented in Section V. A broad discussion is then provided in Section VI. Section VII concludes this research paper and presents the plan for future work.

II. Related Work

There has been a lack of consensus concerning IoT architectural design. Several IoT architectures have been proposed in the literature with different characteristics and properties. A well-known architecture that serves as a reference IoT architectural model is the three-layer architecture [7-9]. It provides a basic architectural design of the IoT functionality with three logical layers, namely the perception, network, and processing layers. A further improvement was made to this basic design to include the application layer at the top level [10-11]. This enables managing IoT services and applications in a more effective way for the end-users.

With the rapid development of IoT, such basic architectures become insufficient to realize the full functionality of IoT systems in an effective manner. They would not be able to efficiently fulfill the different requirements of emerging IoT applications. They can only be feasible at the initial stage of IoT system development. Therefore, other architectures were proposed with additional layers. One is the five-layers architecture which was introduced in [9] to not only realize the structure of loT from a technical point of view but also a business and operational perspective. It incorporates a business layer at the top of the architecture to effectively enable the management of IoT applications based on certain business models and strategies. The other one is the six-layer architecture proposed in [12]. It includes additional layers between the perception and network layers for IoT data monitoring, preparation, storage, and security.

In addition, there have been different proposals focusing on the establishment of specific IoT architectures considering certain common aspects. These include SDN-based implementation [13] security-specific design [14], QoS provisioning [15], and service-oriented perspective [16]. Others focused on certain IoT communication technology such as the architectures proposed in [17] for provisioning 5G-enabled IoT systems. Customized architectures considering specific IoT applications have also been proposed in the literature. These include smart agriculture control [18], tourism management [19], smart metering [20], e-health [21], building automation [22], and water resource management [23]. However, no particular attention has been yet paid to addressing the effective development of an optimized IoT architecture for educational environments.

It can also be seen that these design approaches provide no adequate support for different important aspects. These include the need for security across the different levels of the IoT systems. It is insufficient to address security at a specific layer of the architecture. Security support is critical at the different levels of data acquisition, access, communication, processing, and management. Another important consideration is the incorporation of advanced technologies that would make the deployed IoT system more sustainable. One of these technologies is edge computing which allows the system to be more responsive with very low latency. This is important considering that educational environments are more dynamic and interactive. Another dimension in this context is the need for an effective way to incorporate IoT-based connectivity into these environments. Remote educational areas can be provided with IoT-customized networking support to implement the different IoT applications and services. Therefore, IoT-based network access control is a critical consideration for the effective design of the IoT architecture.

III. IoT Integration in University Systems

For understanding the challenges of integrating IoT into educational environments, we focus in this research work on the specific and demanding case of a university system. It is critical to look into such a complex process at the fundamental level and begin with investigating IoT integration at the infrastructural scale. This would be the initial stage toward the full realization of IoT-based university educational systems. This section presents and discusses the impact of introducing IoT into conventional university systems.

Fig. 1 shows an overview of a typical global university system that incorporates a complex setup of different networking segments, topological entities, interconnections, and computing resources. It has a core infrastructure that interconnects multiple LANs using wired and wireless connectivity. It also has a separate setup for supporting VPN communication with the core system. Internet access is also maintained using a private ISP link. The system also includes a data center having a farm of IT servers for managing different services. These include private servers for web, database, mail, file, and proxy management. Moreover, a set of network entities is used to interconnect the different parts of the system. Different types of switches and routers are deployed in a hierarchical structure. These are core and distributed switches in addition to Internet and local routers implemented at the different levels of the system.

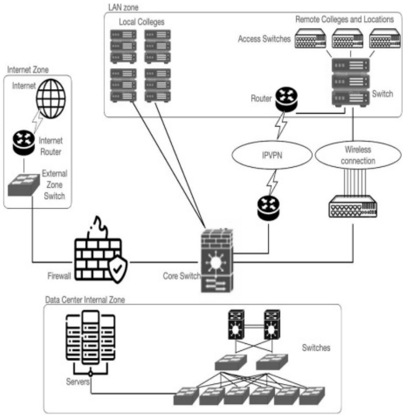

Fig. 1. A Schematic Overview of a Typical Conventional University System.

When the system is integrated with IoT, several IoT-enabling entities need to be introduced to the system. These entities are required to implement the new IoT-related functionalities of the integrated system. For example, IoT sensors and objects are required for enabling IoT data collection and acquisition. Another important functionality is connectivity management and network access control of the IoT devices. This requires special multi-function devices such as IoT gateways with multiple networking capabilities. Furthermore, IoT data in IoT-integrated systems is huge in volume and diversity thus high storage capacities and powerful processing capabilities are highly required. Expanding the current data center with additional IoT servers becomes mandatory. Otherwise, the system needs to be expanded with advanced intelligent computing technologies for effective data management.

It is clear that addressing seamless IoT integration in such systems incurs different challenges. These include the management of heterogeneous IoT devices deployed over vast and maybe remote areas. There is also a need for robust IoT access control considering a variety of IoT communication technologies of distinct properties. Moreover, IoT data management is critical at the different levels of the system. A considerable challenge in this context is addressing big data processing and analytics with a scalable, cost-effective, and flexible solution. Approaching such a challenge using advanced technologies such as cloud computing is the key to efficient and robust IoT data computation and management. Complementing this with the initial processing of the IoT data at the access level would improve resource utilization and performance. However, a trade-off should be maintained between this strategy and the limited capabilities of typical IoT devices at this level of the system. On top of all that, security support is another critical challenging aspect that needs to be fully addressed. Basic security support is insufficient as IoT data need to be secured throughout the different levels of the IoT-integrated system.

IV. Proposed IoT Architecture

The current IoT architectures provide no support for critical advanced aspects as explained in Section II. The importance of these aspects can be seen when considering the complexity and dynamics of the education environments as discussed in the previous section. Taking into account these considerations, a novel IoT architecture is proposed in this section. The following subsections introduce the proposed architecture, present its main components, and discuss potential smart applications.

A. Architecture

The proposed IoT architecture is designed as a multi-layer architecture with the main objective of facilitating the seamless integration of IoT into educational environments. It also aims at optimizing the integrated IoT system with advanced aspects such as complete security support, responsive edge processing, and customized IoT connectivity. The proposed architecture provides a modular, scalable, and simple design that can effectively meet the high volume of IoT data and application demands in the targeted environments.

The proposed IoT architecture consists of six hierarchical layers and one vertical layer. A bidirectional connection flow is established between adjacent hierarchical layers. These are the IoT-object, access, edge-computing, infrastructure, cloud, and application layers that will be discussed in the following sub-section. The focus here is on bridging the gap between IoT and legacy systems in educational environments. It encompasses most of the functionality that is implemented in the legacy systems into the infrastructure layer whereas the other layers facilitate the integration of the distinctive IoT functionalities. The architecture also has a vertical layer for providing complete security support across the different hierarchical layers of the architecture. This layer has a horizontal connection to each other layer to allow securing the system in a comprehensive manner. Fig. 2 shows an architectural representation of the proposed IoT architecture.

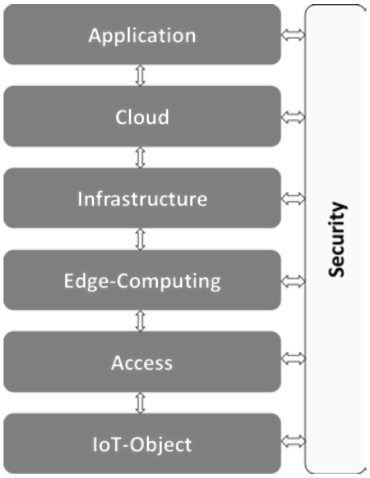

Fig. 2. Architectural Representation of the Proposed IoT Architecture.

The number of layers is selected to ensure effective granularity, modularity, and scalability. That is, each separate and distinctive functionality of the integrated system is embedded in a different layer. This would make IoT integration more simplified and standardized while considering all the essential components of the system. In addition, only the most relevant and critical layers are added to the architecture to maintain a practical trade-off between effective modularity and less complexity. The following part of this subsection describes and discusses each layer of the proposed IoT architecture.

1) IoT-object layer: The bottom layer of the architecture is a physical layer that incorporates all the different IoT objects. These include IoT sensors and actuators in addition to IoT-enabled physical objects. This layer manages IoT data collection and acquisition in addition to controlling requests destined for IoT devices. Furthermore, different aspects including deployment strategy, devices heterogeneity, resource management, and device identification are considered at this level.

2) Access layer: Management of the connectivity of IoT devices with the system is addressed in the access layer. This functionality can be realized using different IoT-based wireless communication technologies. These would include Bluetooth Low Energy (BLE), NB-IoT, 6LowPAN, ZigBee, LoRaWAN, and Sigfox technologies in addition to WiFi and cellular connectivity. This layer controls network access of the IoT devices through different entities such as gateways, aggregators, and access points. It ensures that IoT data collected at the bottom layer is received and delivered to the upper layers for further handling and processing.

3) *Edge-computing layer*: Data transmitted from local IoT subnets through the access layer all the way to further layers can be pre-processed meanwhile. This would enable acting on IoT data at early stages in almost a decentralized manner. Such functionality is realized using the edge-computing layer by initially processing data at different edge nodes such as gateways and local servers. IoT data can be filtered, aggregated, deformed, compressed, and validated for optimized data provisioning and management. Early mining and analysis of the IoT data can also be performed at this layer.

4) *Infrastructure layer*: The core computing and communication of the system is handled at the infrastructure layer. It is the heart of the proposed architecture interconnecting the different parts of the system. The design of this layer enables encompassing and abstracting the core functionality of the university legacy system. This is a key design aspect for facilitating effective integration of the different IoT functionalities into the system.

5) *Cloud layer*: Data management and analysis are realized in this layer with full reliance on cloud technology. IoT data storage and processing are offloaded from the computing infrastructure to the cloud system. The main functionality performed at this layer is effectively managing storage capacities and processing capabilities for IoT data. This requires proper access control to cloud servers and resources. Another consideration in this layer is enabling intelligent IoT data analytics to provide added-value IoT services.

6) *Application layer*: the application layer defines many application-related aspects such as how to utilize the processed data, manage user access to the system, and request IoT services from the underlying layer. Processed IoT data is used at the application layer to produce application-specific services. These can be implemented for different IoT educational applications such as the smart classroom and smart library applications. It is the top layer of the proposed architecture facilitating direct interaction with IoT application users. Therefore, it is responsible for controlling user access to IoT applications and enhancing user experience.

7) *Security layer*: Security management is realized by a vertical layer that is logically interfaced with each level of the architecture. The design of this layer allows incorporating the different security mechanisms into the hierarchy of IoT-integrated systems. These mechanisms include data encryption, user authentication, access authorization, threats isolation, attack detection, and trust control.

B. *Main Components*

To realize the proposed architecture, a set of new IoT elements need to be effectively incorporated into the integrated IoT system. This is presented in Fig. 3 which demonstrates how the legacy university system shown in Fig. 2 can be integrated with IoT. The incorporation of these elements is important to efficiently build up the backbone of the IoT-enhanced university system. Every new element is added to support the functionality of a specific layer. The main elements are presented and discussed in this subsection as follows.

1) *IoT devices*: IoT objects are physical entities embedded with sensors, firmware, processing units, and electronics to enable sensing, sending, and receiving data. IoT devices constitute the main source of data in IoT systems. The most common IoT devices are sensors, actuators, microcontrollers, smart wearables, and wireless cameras. These can be easily provisioned by the proposed architecture at a different scale. The management of these devices is realized at the IoT-object layer to facilitate software/firmware updates, device capability provisioning, and remote diagnostics.

2) *IoT connectivity*: IoT connectivity can be realized using a number of different IoT-oriented connectivity options with distinctive features. They vary in coverage range and power consumption while sharing some properties such as low data transmission rate. These can be classified into short and long-range communication protocols. For example, ZigBee and Bluetooth have short communication ranges whereas LoRaWAN and NB-IoT provide support for long-range communications. The proposed architecture is flexible enough to incorporate different communication protocols and support any potential connectivity requirements. It also supports different communication models such as the point-to-point and point-to-multipoint models. This would enable machine-to-machine communications which allow devices to establish connections among themselves without human intervention.

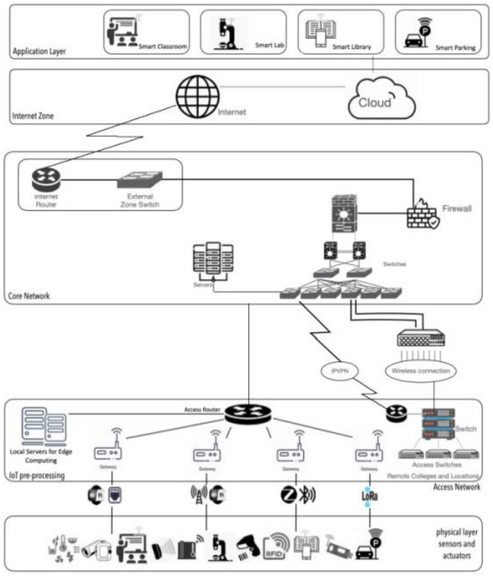

Fig. 3. A Schematic Overview of an IoT-Integrated University System.

3) IoT gateway: Gateways in IoT systems are essential devices to perform different functions. These include IoT data forwarding, protocol conversion, IoT node management, and security support. Gateways are typically deployed at the edge of the IoT network interconnecting IoT nodes to the infrastructure. The network stack of most of the typical IoT devices has no support for IP-based Internet connectivity which can be provided using a gateway. Gateways also provide an additional abstraction to address the heterogeneity and interoperability of IoT devices. In addition, new generation IoT gateways can also provide local caching and pre-processing of IoT data. In the proposed architecture, gateways are essential elements that operate at the access layer to provide all the aforementioned functions. Computing resources of the gateway devices can also be utilized for edge processing at the edge-computing layer of the architecture.

4) IoT edge servers: Edge computing can be realized in IoT systems by deploying edge servers in close proximity to the IoT end nodes. These servers then provide the required computing and storage resources to pre-process IoT data before being transmitted to the cloud. This would help in improving system reliability and availability. Edge servers operate at the edge-computing layer of the proposed architecture with the ability to support a distributed computing model. That is, edge servers deployed across the system can collaborate to provide real-time IoT data pre-processing in a scalable and distributed manner. This is important to improve system responsiveness as the speed and the volume of IoT data is increasing. However, edge servers are usually of limited computing and storage capabilities, unlike the largescale and powerful cloud servers. Therefore, it is critical to have a data management and processing framework to offload computation-intensive data processing to cloud servers.

5) IoT cloud: Cloud computing provides computing resources such as processors, storage, software, and networks as a service. It enables cost-effective data management, on-demand self-service, powerful data computing, and scalability. The proposed architecture enables the development of a cloud-based IoT system to enhance system flexibility and reliability. Relying on the cloud would make IoT integration easier and more effective. It enables unlimited, cost-effective, and on-demand data storage management without any infrastructure limitations and network restrictions. Given that IoT data is typically large and unpredictable, offloading IoT data processing and analytics to the cloud is a feasible strategy to alleviate considerable burdens on the infrastructure.

6) IoT data: IoT data is collected and acquired in different forms and from different IoT objects. These can be status, actionable, location, and automation data in structured and unstructured formats. IoT data is characterized by having a high volume, large-scale streaming, diversity, high dimension, time and space coloration, and high-noise environments. In the proposed architecture, IoT data is handled throughout the different levels of the system. It is collected at the IoT-object layer and then get forwarded at the access layer to the core infrastructure of the system. During that, the data is pre-processed for initial filtration, aggregation, deformation, compression, and validation. Full management and processing of the IoT data are performed at the cloud layer which produces processed application-specific data. Mechanisms and algorithms for data format converting, machine learning, data mining, and reasoning can be performed on IoT data. The basic support that needs to be provisioned for IoT data is storage capacity and processing capabilities.

7) IoT services and interfaces: Once having the IoT-integrated system is established, different IoT services can be provided considering different applications. These services can be developed for different smart activities such as environment monitoring, surveillance, control and automation, face recognition, and productivity support. In addition, IoT users are provided with the required services and interfaces to interact effectively with the system in the context of different IoT applications. All these functionalities are managed at the application layer of the proposed architecture.

C. Potential Smart Applications in Educational Environments

The proposed IoT architecture enables meeting the requirements of different potential smart applications in educational environments. These can include the smart classroom, smart lab, smart library, and smart parking applications. This would facilitate the development of an effective IoT ecosystem that can enhance the teaching-learning process, enrich the educational experience, and improve administrative activities to further limits. This subsection discusses the aforementioned smart applications which can be easily and effectively deployed using the proposed architecture.

All these smart applications require extending the current infrastructure of the university system with additional IoT entities. The proposed architecture supports the effective management of all these entities at the different layers of the architecture. In the smart classroom and lab setups, entities such as environmental and activity sensors, control actuators, and IoT-enabled objects are incorporated. The smart library application would mainly rely on RFIDs technology to tag and manage library resources. For the smart parking application, Infrared and Ultrasonic sensors are used to monitor parking lots. Smart cameras can also be deployed in these applications for smart recognition and AI-based services. For all the different applications, IoT device management is realized at the IoT-object layer.

These IoT devices are mostly main-powered, particularly in the cases of indoor smart applications. Therefore, the connectivity of such devices can be simply maintained using Ethernet and WiFi connections. This would ensure a high data rate and more reliable connections without adhering much to any IoT-oriented concerns regarding energy efficiency. It also makes network access control easier as no additional gateways are required. The proposed architecture also enables implementing IoT devices with other indoor connectivity options such as ZigBee and 6LowPAN if needed. These would be implemented in remote areas where poor or no WiFi coverage exists. In this case, appropriate gateways need to be installed for interconnectivity management with the IP infrastructure. In the case of outdoor smart parking, it is challenging to have accessible Ethernet and WiFi connectivity. Therefore, long-range wireless communication protocols such as LoRaWAN and NB-IoT would be of significant use in these cases. The deployment of a smart parking setup using these protocols requires the provisioning of smart gateways that provides IP interconnectivity. The proposed architecture supports interoperability among all these different communication standards at the access layer.

Massive IoT data streams would be continuously generated in such interactive and dynamic applications. For large-scale deployments in educational environments, the demanding applications of smart classroom and lab would incur a high volume of IoT data. Accordingly, it can highly benefit from edge processing to provide real-time services. Multiple local edge servers can be installed at local LANs to pre-process IoT data streams. Distributed edge processing can also be realized by managing the operations of the widely deployed edge servers using a virtual controller. Such functionality can be practically implemented at the edge-computing layer of the proposed architecture. In the case of the smart parking application, LoRaWAN gateways enabled with the edge computing capability are a feasible solution. It would provide sufficient IoT data handling given the average flow of data in such a predictive application. It is important to note that the proposed architecture supports having both local edge servers and edge-enabled gateways to improve edge computing in the system.

For all the different applications, integrating the IoT ecosystem requires no considerable modifications and updates to the core infrastructure of the legacy university system. The smart classroom application, for example, may only require additional wireless access points to be installed and connected to a local LAN network. Even in the smart parking situation, any installed gateway is interfaced with the core infrastructure through a LAN access router and managed at the access layer of the architecture. In all the different cases, the core infrastructure would only experience an increase in the data rate and may require provisioning more bandwidth for QoS assurance. It though needs no further resource provisioning for data processing and management as the cloud layer is responsible for such functionality.

V. USE CASE

The example presented in Fig. 4 shows an overview of the architectural structure and implementation components of a smart packing application in an educational environment. It demonstrates how the core computing infrastructure is seamlessly integrated with the IoT resources and functionality. The proposed architecture enables a seamless deployment strategy. It starts by connecting the core domain to the access and edge computing domains on one side while being interfaced with the cloud domain on the other side.

Only gateways with average computing resources are installed for each parking block to manage network access of smart parking sensors. LoRaWAN is the feasible connectivity option in this case considering that no easy access to local LANs would be available in outdoor areas. LoRaWAN-enabled sensors and gateways are deployed as needed to have full coverage. On the other hand, smart gateways can be used to provide sufficient resources for pre-processing IoT data traffic streams. That is, streamed data in this case is typically received at average volume from the smart parking sensors. Only very basic sensor data indicating basic information such as the occupancy state of a parking lot is streamed in a textual format. Data can be filtered and aggregated while being timestamped at the edge-computing layer before being forwarded further to the cloud. However, car plate recognition can also be implemented to receive images from smart cameras at the entrance of a parking zone. For such a demanding AI-based service, intensive processing is performed at the cloud servers. At the top layer, smart parking services are provided using interactive user interfaces which are connected to back-end cloud servers.

Cross-layer implementation of full security support is achieved using different security mechanisms. These include but are not limited to authentication, authorization, encryption, and trust management. However, the system is scalable enough to implement additional security solutions at the different levels of the architecture. It is evident that the proposed architecture succeeds in guiding system construction and enhancing the adoption of the smart parking application. Seamless and flexible integration of the introduced IoT resources and functionality was achieved effectively in a plug-and-play fashion.

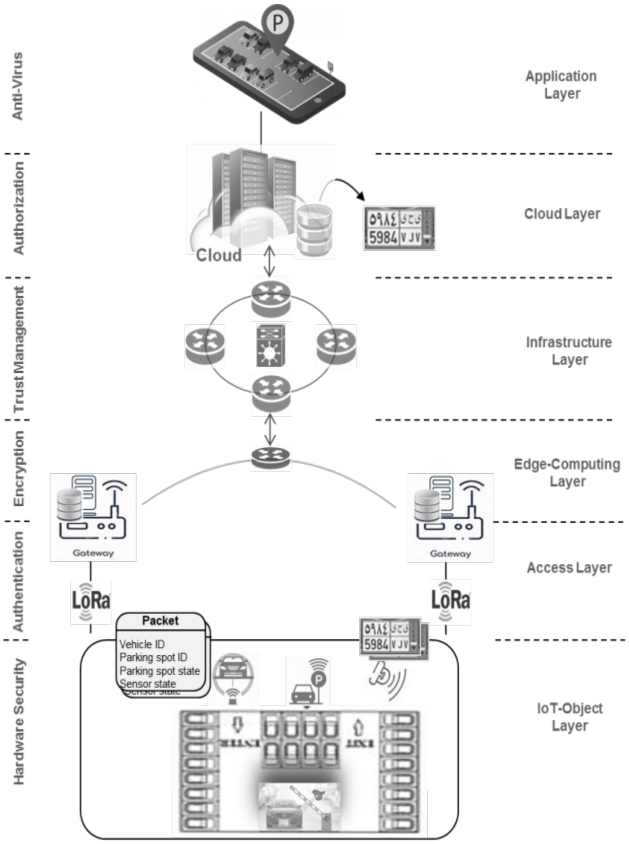

Fig. 4. Overview of a Simple use Case of a Typical Smart Parking Deployment.

VI. Discussion

It can be seen that one of the distinctive properties of the proposed architecture is the split of the networking functionality into two different layers: the access and infrastructure layers. Given the key role of networking support in any IoT-based system, this strategy is important to simplify the integration of IoT communications into the core networking infrastructure of conventional systems. IoT comes with different network access models that are managed at a separate level of the system. Isolating access control would enable effective connectivity among IoT devices and seamless transmission of IoT data over to the core network system.

In addition, the proposed architecture realizes the importance of edge computing for optimizing the responsiveness of the IoT-based system. By placing data pre-processing closer to the physical layer, it ensures that unacceptable latency is considerably alleviated irrespective of the expected high volume and dynamics of IoT data. Having IoT data handled closer to IoT end devices in the system would also improve data management and quality. Real-time processing becomes easy to implement for providing a variety of time-sensitive IoT services. Moreover, such a strategy helps in realizing more advanced support regarding different networking aspects such as user mobility and context-aware smart services.

Another important feature of the proposed architecture is encapsulating most of the functionality of the conventional systems into the infrastructure layer. This also includes all the networking entities and computing resources that constitute the core of these systems. Such a design approach would abstract the core functionality of the existing systems from the IoT integration process and avoid getting into the system complexity. This would be further enhanced with the reliance on cloud computing to realize effective IoT data management and processing. Accordingly, the proposed architecture emphasizes the importance of incorporating the cloud layer to achieve better reliability and less complexity. Furthermore, having a security layer that is interconnected to the whole system ensures the ability to provide complete security support. This design principle of the proposed architecture enables providing the different security services required at each layer.

Table I provides a comparison of the proposed IoT architecture against a set of different architectures. The inherent properties of the proposed architecture can meet different requirements that are critical to university systems. Compared with the other architectures, it provides a salable and modular design that allows elastic expansion of resources and entities to meet different IoT application requirements. It can also grow hierarchically into a different model incorporating other technologies. For example, the architecture can be adapted to accommodate the Blockchain technology in an additional sub-layer or instead of the cloud layer to realize a more decentralized data storage and processing. Encapsulating and abstracting the core computing and communication of the IoT-transformed system into the infrastructure layer makes the architecture more flexible for adaptation.

TABLE I. IoT Architectures Comparison

Architecture	**Scalability**	**Data Management**	**Security Support**	**Responsiveness**	**Wide IoT Coverage**	**Complexity**
[7]	L	L	L	L	L	L
[9]	L	M	L	L	L	L
[10]	M	M	L	L	L	M
[12]	M	M	M	L	L	M
The Proposed Architecture	H	H	H	H	H	M

Compared with other basic architectures, the complexity of the proposed architecture is maintained at an acceptable level given the provisioned set of functionalities. Every layer of the architecture provides essential support to facilitate IoT integration and enhance the IoT system. Having a vertical layer for full security provision would add to its complexity but at the benefit of providing significant support of security at each level of the architecture.

VII. Conclusion

Seamless integration of IoT in legacy university systems is still a considerable challenge. The proposed architecture in this paper efficiently addresses such a challenge to facilitate IoT integration and accelerate IoT adoption. It comes with a modular and scalable design allowing the effective abstraction of the legacy infrastructure of the university system. It is based on a seven-layer model that incorporates advanced technological considerations including combined edge-cloud computing in addition to effective IoT accessibility. In addition, the architecture is optimized toward complete security support using a vertical layer covering the whole system. It also provides responsive edge processing to support real-time communication with low system latency. The architecture also supports customized IoT connectivity and simplifies the deployment of heterogeneous IoT communication technologies. In comparison with other IoT architectures, the proposed one ensures high reliability, data management, security support, responsiveness, and wide coverage while maintaining acceptable complexity. The focus of the future work will be on studying how the proposed architecture can be extended to other specific IoT use cases. Another aspect that will be investigated is incorporating other technological advances such as Blockchain technology.

References

[1] M. Selinger, A. Sepulveda and J. Buchan, "Education and the Internet of Everything", Cisco Consulting Services EMEAR Educational Team, October 2013, [online] Available: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/education_internet.pdf.

[2] S. Selvaraj and S. Sundaravaradhan, “Challenges and opportunities in IoT healthcare systems: a systematic review,” SN Applied Sciences, vol. 2, no. 1, pp. 1-8, 2020.

[3] B. Chandrayan and R. Kumar, “IoT integration in industry—a literature review,” Recent Advances in Mechanical Engineering, pp. 9-17, 2020.

[4] J. Ruan, J. Hua, Z. Chunsheng, H. Xiangpei, S. Yan, L. Tianjun, R. Weizhen, and C. Felix, “Agriculture IoT: Emerging Trends, Cooperation Networks, and Outlook,” IEEE Wireless Communications, vol. 26, no. 6, pp. 56-63, 2019.

[5] M. Al-Emran, S. I. Malik and M. N. Al-Kabi, "A survey of Internet of Things (IoT) in education: Opportunities and challenges" in Toward Social Internet Things (SIoT): Enabling Technologies Architectures and Applications, Cham, Switzerland:Springer, pp. 197-209, 2020.

[6] B. Dhanalaxmi and G. A. Naidu, "A survey on design and analysis of robust IoT architecture," in International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2017, pp. 375-378.

[7] I. Mashal, O. Alsaryrah, T.Y. Chung, C.Z. Yang, W.H. Kuo, and D.P. Agrawal, “Choices for interaction with things on Internet and underlying issues,” Ad Hoc Networks, vol. 28, pp. 68-90, May 2015.

[8] O. Said and M. Masud, “Towards internet of things: Survey and future vision,” International Journal of Computer Networks, vol. 5, no. 1, pp.1-17, 2013.

[9] M. Wu, T.J. Lu, F.Y. Ling, J. Sun, and H.Y. Du, “Research on the architecture of Internet of Things," in the 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010, pp. V5-484-V5-487.

[10] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey,” Sensors, vol. 18, no. 9, p. 2796, Aug. 2018.

[11] N. V. Lopes, F. Pinto, P. Furtado and J. Silva, “IoT architecture proposal for disabled people,” in IEEE 10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2014, pp. 152-158.

[12] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 2017.

[13] K. K. Karmakar, V. Varadharajan, S. Nepal and U. Tupakula, "SDN-Enabled Secure IoT Architecture," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6549-6564, April 2021.

[14] R. T. Tiburski et al., "Lightweight Security Architecture Based on Embedded Virtualization and Trust Mechanisms for IoT Edge Devices," in IEEE Communications Magazine, vol. 57, no. 2, pp. 67-73, February 2019.

[15] N. Lo and I. Niang, “A Comparison of QoS-Based Architecture Solutions for IoT/Edge Computing Environment,” Emerging Trends in ICT for Sustainable Development, pp. 355-364, 2021.

[16] S. Maurya and K. Mukherjee, “An energy efficient architecture of IoT based on service oriented architecture (SOA),” Informatica, vol. 43, no. 1, pp. 87–93, 2019.

[17] H. Rahimi, A. Zibaeenejad and A. A. Safavi, “A Novel IoT Architecture based on 5G-IoT and Next Generation Technologies,” in IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 81-88.

[18] S. Verma, R. Gala, S. Madhavan, S. Burkule, S. Chauhan and C. Prakash, “An Internet of Things (IoT) Architecture for Smart Agriculture,” in 4th International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1-4.

[19] M. Nitti, V. Pilloni, D. Giusto, and V. Popescu, “IoT Architecture for a Sustainable Tourism Application in a Smart City Environment,” Mobile Information Systems, vol. 2017, Article ID 9201640, 2017.

[20] J. Lloret, J. Tomas, A. Canovas and L. Parra, “An Integrated IoT Architecture for Smart Metering,” IEEE Communications Magazine, vol. 54, no. 12, pp. 50-57, December 2016.

[21] O. Debauche, S. Mahmoudi, P. Manneback, A. Assila, “Fog IoT for Health: A new Architecture for Patients and Elderly Monitoring,” Procedia Computer Science, vol 160, pp. 289-297, 2019.

[22] D. Sembroiz, S. Ricciardi, D. Careglio, “A Novel Cloud-Based IoT Architecture for Smart Building Automation,” Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, Eds.; Academic Press: Cambridge, MA, USA, 2018; pp. 215–233.

[23] M. Muñoz, J. Gil, L. Roca, F. Rodríguez, and M. Berenguel, “An IoT Architecture for Water Resource Management in Agroindustrial Environments: A Case Study in Almería (Spain),” Sensors, vol. 20, no. 3, p. 596, Jan. 2020.