Determinants towards a Better Acceptance Model of IoT in KSA and Eradication of Distrust in Omnipresent Environments

Abdulaziz A. Albesher[1]
College of Computing and Informatics
Saudi Electronic University, Riyadh, Saudi Arabia

Adeeb Alhomoud[2]
College of Science and Theoretical Studies
Saudi Electronic University, Riyadh, Saudi Arabia

***Abstract*—This paper highlights several of the key determinants that play a vital role in the acceptance of Internet of Things (IoT) technologies in the Kingdom of Saudi Arabia (KSA). Based on the governmental focus towards technology and the response of the citizens towards embracing new technologies, several determining factors are presented. Certain essential application areas of IoT are analyzed including the local industry, agriculture and livestock, health, education, smart metropolitans and smart government. In addition, we also explore acceptance at the personal level, such as home and privacy of individuals, security, and personal management with IoT wearables. Towards the end of this paper, some challenges of the IoT acceptance are presented along with the analysis of key enablers. All the rationalizations lead to the conclusion that IoT acceptance is inevitable based on the number of associated benefits which will enhance once the posed challenges are addressed.**

Keywords*—*Internet of Things (IoT); security; health; IoT acceptance; smart cities

I. Introduction

The Internet of Things (IoT) is one of the most accelerated emerging technologies that is perceived to be widely spread in the coming decade [1]. It comprises of an expanding network of smart devices that are capable of communicating over the internet and use various network services to interact with other internet-enabled devices. IoT is being applied in various domains including health and medical care [2], smart organizations [3], smart homes, smart cities, agriculture [4], e-commerce and personal management, to name a few. In addition, it is expected to be a catalytic agent for a variety of other advancements such as upgrading of the existing broadband networks [5], advancement in sensor technologies, longer battery life, emergence of situation-aware [6] and business-aware organizational networks [7], and many more like the same. It is estimated that the number of IoT-enabled devices connected to the internet would reach over 43 billion by 2023 [8]. There are a number of benefits with the emergence and blending of IoT technologies in our daily lives. In the corporate world, IoT is an enabler for business digitalization strategies [9]. Data gathered from the IoT devices is highly useful for analyzing consumer behavior, choices, consumption and attitudes. This can increase a company's competitive advantage by transforming its services and products into higher amplifications that are never seen before. Likewise, IoT is transforming the agricultural economies of the world by employing online monitoring, efficiency, cleaner processes, reduced resources and greenhouse automation for better crop yield [10]. IoT is also adopted for automating several of the civic amenities in smart cities [11]. In smart homes and buildings, IoT contributes to facilities management, energy management, occupants and resources tracking, and comfort enhancement. On the frontiers of health and automatic disease classification [12], IoT has bolstered through the concepts of ambient-assisted living, wearable devices, internet of mobile things and similar health information systems [13][14]. In the education sector, IoT has influenced with sensors, intra-communication among wearable technologies, augmented reality and cloud computing for assisted and remote learning [15].

Along with many potential benefits, there are several risks and elements of distrust associated with IoT, which hinders the acceptance of IoT at the personal and national levels. The first and the foremost risk element associated with IoT is the security of the data. As presented in a recent survey [16], a large number of IoT devices are still prone to hacking. As IoT technologies provide communication and access on-the-go, privacy of the individuals is also at higher stake. This leads to a distrust in the technology and could also pave path to the rights infringement [17]. In addition, some IoT environments also pose threats to health via excessive radiation [18].

Based on these potential benefits and associated risks perceived by the masses, countries around the world face reluctance and insecurity in the acceptance of IoT technologies. There have been several models discussed in literature for IoT acceptance. Some prominent models among these include Technology Acceptance Model (TAM), Theory of Reasoned Action (TRA) [19], and Structural Equation Model (SEM). In order to appropriately utilize any of these models, it is equivalently important to select the right set of attributes which are deterministic.

In this work, we exploit several of the determinants that play a critical role in IoT adoption and in structuring of a model that is highly judicious for IoT acceptance in the Kingdom of Saudi Arabia (KSA). Based on extensive literature survey, we investigate several key application areas of IoT, which include acceptance at the national level, such as in the industry, health, education, civic amenities and agriculture. In addition, we explore acceptance at the personal level, such as home and privacy of individuals, security, and personal management with IoT wearables. Towards the end of this study, we highlight some of the enablers of IoT acceptance and various challenges faced that can hinder its acceptability.

The rest of the paper is organized as follows. Section 2 discusses the factors affecting IoT acceptance in the economic and societal sectors in Saudi Arabia. It also presents and analyzes some of the determinants that contribute to the acceptance of IoT at the personal levels. Section 3 discusses IoT acceptance enablers and the challenges that hinder the potential growth in KSA with the implementation of IoT. Conclusions are presented in Section 5, followed by the references.

II. IoT Acceptance at the National Level

There are a number of application areas of IoT at the national level in KSA. We segregate them in to five major areas including industry, agriculture, health, education and civic amenities. The following subsections highlights the key determinants of IoT acceptance in these areas.

A. *IoT in Industry*

The industrial sector of any country is one of the foundation pillars that bear the weight of major economic growth. There are several benefits pertaining to IoT integration that motivates its acceptance in the industrial and corporate organizational setups in KSA. Owing to the fact that IoT technologies dispense a two-fold communication possibility by providing people-to-things as well as things-to-things communication, its adoption in the industry is highly desired. From the point of view of industrial ecosystem [20], IoT could prove to be a central part that is enticing for the ecosystem actors to engage with. These actors, or determinants, may include:

- Supply Network: The products and services offered by a specific industry. It could be in the form of knowledge, services or goods.
- Influencers: Experts, standards alliances, industry associations, social media bloggers, journalists, worker unions etc. who can influence IoT acceptance.
- Complementors: The additional services or products offered along with the supply network.
- Intermediaries: Retailers, distributors and similar entities that facilitate the business and acts as a bridge between the industry and the end users.

In addition to these, IoT technologies are particularly very beneficial in implementing industrial safety. Industrial accidents can lead to crucial loss of human life and expensive equipment. There are a variety of sensors and actuators that are eminently useful for maintaining safety and high standards in industrial production environments. These include sensors for measuring temperature, touch, pressure, humidity, smoke, proximity, gas leakage, to name a few. Likewise, distances can be detected and accidents can be prevented using various ultrasonic and infrared sensors.

Through Wireless Body Area Networks (WBANs) [21], employees' health can be continuously monitored. Any ailment, lack of conscience or abrupt changes in vital measurements such as blood pressure, heart rate or glucose levels can be communicated to a centralized system for responding and taking preventive measures.

Other determinants of IoT acceptance in the industry pose various kinds of challenges such as devices challenges, network challenges and data challenges [22]. Devices in a network may have different capabilities and communicate over different protocols. These capabilities are both related to the hardware and the software. Non-standardized naming of devices in a network is another challenge. The integration of cloud computing with IoT expands the operating scale of industrial applications. Data in the industrial application of IoT can be categorized as (1) Data by the things, such as the values of temperature, distances, pressure, etc.; and (2) Data about the things, such as IDs, names, addresses, types etc. One of the examples of such application is in churn prediction [23]. The huge amounts of data generated from the IoT-enabled devices helps in better analysis to predict users likely to churn. Hence, the industrial acceptance of IoT is largely dependent on the afore-mentioned determinants that play a vital role.

B. *IoT in Agriculture and Livestock*

Like all the major countries of the world, KSA also produces most of the food indigenously, besides lack of water and extremely hot and dry climate. In circumstances such as these, IoT is a promising technology for the growth of agriculture in terms of yield, crop management and disease eradication. Data is gathered and shared over the network using a number of different sensors such as soil sensors, leaf sensors, stem sensors, roots sensors, temperature, humidity and fruit size sensors [24]. Besides these sensors, precision based devices such as drones and robots are also utilized for smart and precision agriculture.

There are a number of enablers that determine the use and acceptance of IoT technologies in agriculture and livestock. These include soil and water quality monitoring, farm monitoring, irrigation and nutrition management, disease and pest monitoring, crop health monitoring, cattle movement and management, controlled use of fertilizers, farm assets tracking, and intelligent greenhouses [10]. Fig. 1 shows a typical scenario of a farm area network based on IoT.

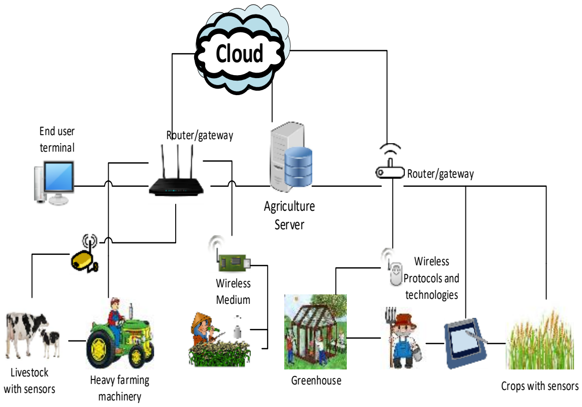

Fig. 1. A Typical Farm Area Network based on IoT Technology.

Referring to the scenario of KSA, there a number of application areas that can highly benefit from IoT technologies, thus indicating the likelihood of its immediate acceptance. These include:

- Irrigation.
- Fertilizer Management.
- Soil sampling and mapping.
- Pest management and disease control.
- Yield monitoring and harvest forecasting.
- Farm management.
- Cattle produce management.

Apart from huge potential of IoT in agriculture sector, there are a number of challenges. These include the network and hardware challenges, sensors and battery life, architectural platform differences, interference, reliability and scalability of IoT based networks. These challenges are also key determinants in IoT acceptance in the agricultural sector in KSA.

C. IoT in Education

During the recent outbreak of COVID-19 pandemic, almost all of the educational institutes around the globe either suspended their educational services or shifted to online education. It is evident that IoT technologies possess a great potential to be used in a variety of ways in order to help both the teachers and learners at the same time. One of the prime determinants in its acceptance is the enhanced learning and teaching experience derived from the analysis of data collected from various devices and sensors. Among many possibilities of enhancement of the education sector with IoT in KSA, some of the prime benefits are reducing the dropout rate in the examination through superior learning experience, achieving the learning objectives with ease, and improving the overall operations of the institutions.

The three essential skills devised for the students in the 21st century include learning and innovation skills, life and career related skills, and information technology skills [25]. IoT introduces technologies to the students, which highly inculcate in-depth understanding of the subjects of study, as well as allows their continuous physiological and behavioral monitoring. The data gathered from this can be used to design learning pedagogies that yield maximum learning capabilities with ease and less physical and mental strain.

Based on the importance of several possible factors that contribute to the overall education ecosystem improvement with the use of IoT, the following are some of the most significant determinants for IoT acceptance in education:

- Trust: A trustworthy and reliable security and privacy mechanism is needed that is readily embraced and poses no infringements of learners and educators security and privacy.
- Cost: The associated cost of the IoT adoption is anticipated to be less as compared to the expected gain. A higher cost could lead to hindrance in the acceptance of IoT.
- Expected Performance Elevation: The trust level of a user that by embracing IoT, the overall performance would be elevated.
- Expected Effort (ease of use): The amount of effort and time spent in learning new IoT enabled technologies and adapting it. It is anticipated that with technologies like online learning management systems and virtual classrooms, time and effort spent in travelling and coping with the distances will be highly reduced.
- Social Influence: One of the prime factor in acceptance of IoT is how society and influencers, such as prominent personalities, government agencies and social media, react to it. The more welcoming the response would be from these actors, the higher would be the acceptance rate of IoT in KSA.
- Hedonistic Motivation: The overall experience of learning and teaching with IoT technologies is desired to increase the pleasure in learning such as to increase motivation towards learning. The higher the pleasure level, the greater are the chances of acceptance.

The above mentioned factors also possess a number of associated challenges and risks. For the acceptance of IoT, these challenges need to be addressed and risks to be mitigated [26].

D. IoT in Health

With the transformation of the wireless sensor networks into IPv6 based lower power wireless personal area networks (6LoWPAN), smallest of the devices, with inadequate processing capability and battery-life, can transmit information wirelessly over the internet. One of the appreciable implementations of these in the medical sector is in the form of smart wearables capable of measuring and communicating vital health indicators to a centralized health monitoring system, which is connected to a hospital or other emergency medical service providers. There are a considerable number of application areas of IoT in the health sector. Some of the most prominent ones include diagnostics, counselling and therapy, drugs reference, clinical communications and medical application.

With these potential benefits, there are some associated risks of IoT adoption. One of the most prominent risk factors is the security of patient's information and privacy of the data. A slightest modification of the data due to any illegitimate infringement could result in a life-and-death scenario. Other factors affecting the acceptance of the IoT devices include the precision of the sensors and electronic measurement devices, the cost of the devices, ease of use, and the battery life.

E. IoT in Smart Cities

The adaptation of IoT technologies and the availability of devices and sensors communicating among them creates an ecosystem, which leads to smart cities. Smart cities use smart things to carry out various civic functions automatically such as efficient utilization of energy, traffic control, emergency management, smart transportation and ride sharing, lighting control, health and pollution monitoring, and surveillance [27].

Like other metropolitan cities of the world, KSA has many big cities with high population. They can receive deterministic benefits from IoT technologies in a number of ways. One of the most significant data to manage could be the traffic data. With appropriate analysis of this data, municipal governments and citizens can take a number of benefits ranging from traffic management and congestion control, efficient utilization of available parking spaces, logistics management, to better utilization of urban transport systems.

Another area where the data gathered through IoT devices could play a significant role is in surveillance of the modern cities. During the past two decades, the world has witnessed major terrorist activities around the globe. Most of these activities were carried out on public places. With smart systems capable of detecting anomalies using widely spread camera networks, terrorists' activities and other crimes can be efficiently monitored.

Smart cities also provide better means of pollution control and resource management. Water and energy can be efficiently managed and consumers can be billed with different customized option through the data gathered via smart metering. This benefits both the government, in terms of efficient resource utilization, as well as the citizens, in terms of customizable utility option that minimizes bills.

Another very important factor that contributes to IoT acceptance is the transformation of ordinary infrastructures into smart homes [28], offices and buildings. Various IoT enabled sensors and devices are highly useful in improving the everyday life and freeing up residents to perform other responsibilities. These include sensors based systems for automatic security and surveillance of buildings, efficient utilization of resources such as electricity and water, and emergency management systems that are connected to the hospital, police and fire departments. Recent state of the art systems are also capable of checking and maintaining building health and environment.

Along with the aforementioned deterministic benefits of IoT acceptance, there are several challenges that are of consideration. One of the biggest challenges is the quality of data and its integrity. IoT technologies are still novice and a lot of enhancement and improvement is required to assure complete data integrity with highest quality. Another important challenge is of the management and coordination of various systems in the IoT-based smart cities. The massive and speedy spread of IoT in businesses, homes, social settings and other kinds of environments require equivalent management and coordination speed. These areas are evolving and still needs a lot of improvement. Another notable challenge is of efficient use of energy by the IoT-enabled devices. Most of the sensors depend upon batteries as their sole source of energy. Efficient use of energy and the battery technologies have also improved in the last decade and still further research in these areas is required. Fig. 2 demonstrates the importance of IoT in smart cities.

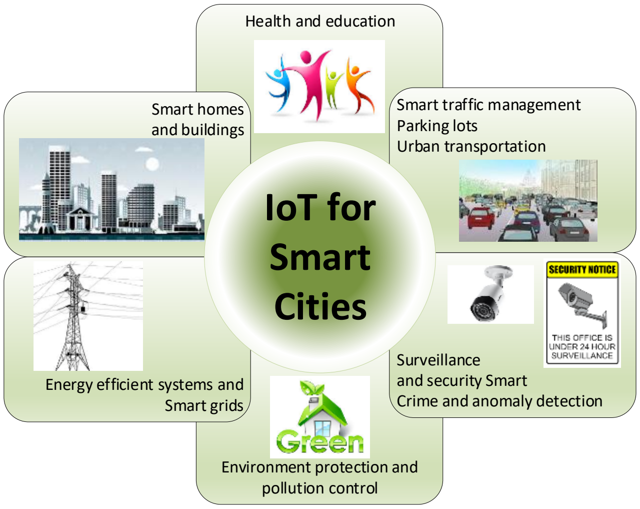
Health and education
Smart homes and buildings
Smart traffic management
Parking lots
Urban transportation
IoT for Smart Cities
SECURITY NOTICE
THIS OFFICE IS UNDER 24 HOUR SURVEILLANCE
Energy efficient systems and Smart grids
Surveillance and security Smart
Crime and anomaly detection
Green
Environment protection and pollution control

Fig. 2. The Role of IoT in Smart Cities.

F. *Personal Management with IoT-Enabled Wearables*

The success of IoT acceptance does not imply on the national level alone, rather, it is greatly influenced by the acceptance at the individual levels. One such example of the benefits of IoT in the personal lives of individuals is Amazon Echo, which is a voice-based interface for physically impaired people. It allows them to control several IoT devices in the home and perform daily activities with more ease.

There are a myriad of applications for personal management and monitoring comprising different IoT-enabled devices and sensors. One major application is in the health area. Smart health wearables keep a track of vital health related measurements including the heart rate, blood pressure, glucose levels etc. Special sensors and designed devices help people with different types of impairments, such as visual, cognitive, auditory or mobility impairments, in their daily activities. Fitness bands helps in monitoring a number of activities, such as the distance travelled, the number of steps taken, and the calories burnt etc. in a specified length of time.

Other prevalent use of IoT at the personal level is in the form of digital assistants. Devices and systems are capable of performing a number of assistance level activities in daily chores of individuals. Some of the examples include Amazon Alexa, Google Home, Siri, Wink and SmartThings [29]. These are Artificial Intelligence (AI) assisted products that are capable of working on voice commands and take care of trivial and advanced tasks from switching on/off the lights to scheduled maintenance of the house and taking care of the personal schedules.

Agile technology companies around the globe have started developing their products in a way that implicitly supports IoT way of life. One of the pertinent examples is the Apple's strategy and gambit that their phone work best when paired with any of the other Apple's wearable devices such as their smart watch [30]. In a recent Consumer News and Business Channel (CNBC) survey of 2017, the average American household owns at least two or more Apple products [31]. Allusive Market moves such as these paves the path to citizens tacitly embracing the IoT technology and blending it into their daily lives. Thus, contributing to the perceived and actual usefulness of IoT technology at the personal levels.

Besides all the aforementioned advantages, there a number of challenges with the use of IoT at the personal level. The first and the far most matter of concern is the security and reliability of IoT-enabled devices. Account lockout, weak passwords and illegitimate attacks mounted on poorly encrypted data pose a lot of threat to the personal data. Lack of standards play a vital role in this and efforts are being made to unify these.

III. IoT Acceptance Enablers and Challenges

Based on the discussion presented in the previous sections, we highlight, in this section, the key challenges faced by IoT adoption and present some of the main enablers of IoT acceptance that can overcome and mitigate some of the hindrances. Table I shows some of these challenges. The primary issues include:

- Security: Since the IoT technologies are still in infancy, they are subjected to a number of hostile attacks. These attacks could be targeted illegitimate, or by mistake as well, such as a device failure network scan-based random attacks. Such threats in the security of IoT devices and networks could be very dangerous in some applications such as medical, traffic control and home applications. The security threats in IoT can be classified into three categories, namely, (i) perception level (device level), (ii) transition level (network level), and (iii) application level (data level).
- Privacy: Privacy is also a major concern and contributes a lot towards the trust factor in IoT technologies along with the security factor. Privacy is further at risk when IoT devices communicate in open networks and premises are shared among residents. Research on de-anonymization techniques in the context of IoT can be very helpful.
- Trust: One of the most difficult hurdle to introduce a new technology is the trust factor of the masses. A trustworthy and reliable security and privacy mechanism is needed that is readily embraced and poses no infringements in the privacy and security of individuals. Also, there is a lack of trust when the technology has the capability of replacing humans and taking the full control over the systems.
- Scalability: The current state of the art technologies in IoT needs to incorporate the element of scalability in order to be implemented on a national scale. For this, IoT-enabled device manufacturers and service providers need to improve the quality of services, increase marketing speed, and reduce development costs. Better and new models for communication with low power consumption need to be developed instead of the client-server model existing in the most communication networks today. In addition, interoperability of devices is also very necessary in order to achieve scalability.
- Cost: In order to make it widely adopted and acceptable as a scalable technology, the cost of the IoT based devices and network components and sensors need to be minimized. The associated cost of the IoT adoption is anticipated to be less as compared to the expected gain. A higher cost could lead to hindrance in the acceptance of IoT.
- Standardization: IoT devices are manufactured by different vendors and there is a lack of common standards, especially when it comes to the communication protocol. The communication technologies between these devices also vary, for example, Blue Tooth, WiFi, IEEE 802.15.4, etc. This also makes the security among devices difficult to be maintained.
- Data Collection and Storage: With IoT technologies in practice, the amount of data is expected to explode beyond any leaps and bounds. Not only the storage and collection of such a large amount of data is an issue, the heterogeneity of the data poses greater challenge. Technologies like cloud computing and fog computing have greatly contributed to providing IoT technologies with the ability to cope with such large amounts of data.

Table II presents some of the enablers of IoT acceptance that are highly beneficial in the adoption of IoT on a national as well as personal scale in KSA. Among these the first and the far most important factor is related to the governance of IoT technology by laying down the basic rules and principles governing the IoT implementations [32]. The second important aspect is following acceptable standards for IoT implementation and continuous monitoring and analysis of these standards in collaboration with all the stakeholders. These stake holders can be from the public or private sectors. Therefore, the partnership between the public and private sectors also plays a very vital role in IoT adoption and the government, with the help of the private sector, can initiate joint projects.

TABLE I. IoT Acceptance Challenges in KSA

IoT Challenges	Description
Security	IoT-enabled devices and networks are still subjected to a number of legitimate and illegitimate attacks
Privacy	Devices communicating over open network pose a large threat to privacy of individuals and organizations
Trust	Lack of security, privacy and the capability of devices taking over the system leads to distrust
Scalability	Interoperability, speed in marketing and low cost is needed to achieve scalability in IoT technologies.
Cost	Cost of the current devices, sensors and the network components needs to be reduced
Standardization	Different vendors have their own standards, operating systems, hardware and communication protocols. The need for developing standards is demanded.
Data Collection and Storage	The amount of data generated with so many devices and sensors is huge. Proper mechanisms are needed to handle, store and analyze this huge data.

TABLE II. ENABLERS OF IOT TECHNOLOGY ACCEPTANCE IN KSA

	IoT Enabler	**Description**
1	Governance	Laying down the basic rules and principles governing the IoT implementations
2	Standardization	Continuous monitoring and analysis of IoT standardization process.
3	Public-Private Partnership	Joint projects can be initiated by the government with the help of the private sector
4	Awareness campaigns for the masses	A comprehensive campaign for the awareness of the masses, including the industrial workers and home users.
5	Initialization of pilot projects	Pilot projects must be initialized to pave path towards stepwise adoption and innovation in the existing technologies according to the societal needs
6	Catalyst for economic growth and better society	IoT can be considered as an important factor for the economic growth and evolution of the society.
7	Continuous Research and Development	Continuous research and development initiatives and support should be provided for implementing and developing IoT technologies enhancements
8	Protection of privacy	Protection of personal and organizational privacy should be ensured and appropriate amendments and enhancements in the law should be made when necessary
9	Right to disconnect	The users of the IoT networks should have the right to be disconnected and conceal their identities.
10	Emerging risks identification and mitigation	Emerging risks should be identified and countermeasures should be established to deal with the surfacing risks to privacy

For the awareness of IoT in the masses, a comprehensive campaign is needed that includes meetings with the industrial workers and home users. Another enabler is the initiative to initialize pilot projects at different levels. Pilot projects pave path towards stepwise adoption and innovation in the existing technologies according to the societal needs. Thus, enabling IoT as a catalyst for the economic growth and the evolution of the society. Therefore, Continuous research and development initiatives and support should be provided for implementing and developing IoT technologies enhancements.

Protection of privacy of individuals and organizations is another enabler of IoT adoption. Privacy protection should be ensured and appropriate amendments and enhancements in the law should be made when necessary. The users of the IoT networks should have the right to be disconnected and conceal their identities. In addition, Emerging risks should be identified and countermeasures should be established to deal with the surfacing risks to privacy.

IV. CONCLUSION

This work provides an insight to the primary determinants of the acceptance of IoT in the KSA. It highlights several application areas at the national as well as the individual levels. These include the acceptance in the industry, agriculture and livestock, education, health, smart cities, personal management with IoT enabled wearables, and AI assisted technologies. Along with the potential benefits that contribute to the acceptance and perceived acceptance of the technology, there are a number of risks that are identified. These challenges include security and privacy of IoT, trust, cost of devices and components, scalability, standardization, and data collection and storage issues. IoT can be a way of life where its proper acceptance require mitigation of these issues. Lastly, this work highlights some enablers that could contribute to the swift acceptance of IoT technologies in KSA.

ACKNOWLEDGMENT

The authors highly acknowledge the financial support provided by the Deanship of Scientific Research (DSR) at Saudi Electronic University, Saudi Arabia to publish this research.

REFERENCES

[1] H. Lee, “Home IoT resistance: Extended privacy and vulnerability perspective,” Telematics and Informatics, vol. 49, p. 101377, Jun. 2020, doi: 10.1016/j.tele.2020.101377.

[2] S. Kim and S. Kim, “User preference for an IoT healthcare application for lifestyle disease management,” Telecommunications Policy, vol. 42, no. 4, pp. 304–314, May 2018, doi: 10.1016/j.telpol.2017.03.006.

[3] P. Brous, M. Janssen, and P. Herder, “The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations,” International Journal of Information Management, vol. 51, p. 101952, Apr. 2020, doi: 10.1016/j.ijinfomgt .2019.05.008.

[4] R. Pillai and B. Sivathanu, “Adoption of internet of things (IoT) in the agriculture industry deploying the BRT framework,” Benchmarking: An International Journal, vol. 27, no. 4, pp. 1341–1368, Jun. 2020, doi: 10.1108/BIJ-08-2019-0361.

[5] T. Sudtasan and H. Mitomo, “The Internet of Things as an accelerator of advancement of broadband networks: A case of Thailand,” Telecommunications Policy, vol. 42, no. 4, pp. 293–303, May 2018, doi: 10.1016/j.telpol.2017.08.008.

[6] J. Robert, S. Kubler, and S. Ghatpande, “Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems,” Future Generation Computer Systems, vol. 112, pp. 283–296, Nov. 2020, doi: 10.1016/j.future.2020.05.033.

[7] S. Teixeira et al., “LAURA architecture: Towards a simpler way of building situation-aware and business-aware IoT applications,” Journal of Systems and Software, vol. 161, p. 110494, Mar. 2020, doi: 10.1016/j.jss.2019.110494.

[8] “Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017,” Gartner. https://www.gartner.com/en/documents/3840665/forecast-internet-of-things-endpoints-and-associated-ser (accessed Aug. 26, 2020).

[9] A. Sestino, M. I. Prete, L. Piper, and G. Guido, “Internet of Things and Big Data as enablers for business digitalization strategies,” Technovation, Jan. 2020, doi: 10.1016/j.technovation.2020.102173.

[10] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, “A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming,” IEEE Access, vol. 7, pp. 156237–156271, 2019, doi: 10.1109/ACCESS.2019.2949703.

[11] Z. Khan, A. Anjum, K. Soomro, and M. A. Tahir, “Towards cloud based big data analytics for smart future cities,” J Cloud Comp, vol. 4, no. 1, p. 2, Feb. 2015, doi: 10.1186/s13677-015-0026-8.

[12] I. Usman and K. A. Almejalli, “Intelligent Automated Detection of Microaneurysms in Fundus Images Using Feature-Set Tuning,” IEEE Access, vol. 8, pp. 65187–65196, 2020, doi: 10.1109/ACCESS. 2020.2985543.

[13] A. Albesher, “IoT in Health-care: Recent Advances in the Development of Smart Cyber-Physical Ubiquitous Environments,” IJCNS, vol. 19, no. 2, pp. 181–186.

[14] S. M. R. Islam, D. Kwak, MD. H. Kabir, M. Hossain, and K.-S. Kwak, “The Internet of Things for Health Care: A Comprehensive Survey,”

IEEE Access, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[15] A. Majeed and M. Ali, "How Internet-of-Things (IoT) making the university campuses smart? QA higher education (QAHE) perspective," in 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2018, pp. 646–648, doi: 10.1109/CCWC.2018.8301774.

[16] "The cheap security cameras inviting hackers into your home – Which? News." https://www.which.co.uk/news/2019/10/the-cheap-security-cameras-inviting-hackers-into-your-home/ (accessed Aug. 17, 2020).

[17] T. Naheed, I. Usman, and A. Dar, "Lossless data hiding using optimized interpolation error expansion," in Frontiers of Information Technology (FIT), 2011, 2011, pp. 281–286.

[18] S. Hu, B. Hu, and Y. Cao, "The wider, the better? The interaction between the IoT diffusion and online retailers' decisions," Physica A: Statistical Mechanics and its Applications, vol. 509, pp. 196–209, Nov. 2018, doi: 10.1016/j.physa.2018.06.008.

[19] Jieh-Haur CHEN, Nguyen Thi Thu HA, Hsing-Wei TAI, and Chao-An Chang, "The Willingness to Adopt the Internet of Things (IoT) Conception in Taiwan's Construction Industry," Journal of Civil Engineering & Management, vol. 26, no. 6, pp. 534–550, Aug. 2020, doi: 10.3846/jcem.2020.12639.

[20] R. Gupta, K. Miyazaki, and Y. Kajikawa, "Ingredients of Successful Emerging Business Ecosystems: Case of Industrial IoT Adoption," 2018 Portland International Conference on Management of Engineering and Technology (PICMET), 2018, doi: 10.23919/PICMET.2018.8481854.

[21] R. Gorli, "A New Approach for Employee Safety in Industries with IoT," i-Manager's Journal on Information Technology; Nagercoil, vol. 7, no. 2, pp. 22–29, May 2018, doi: http://dx.doi.org.sdl.idm.oclc.org/10.26634/jit.7.2.14650.

[22] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial internet of things: A comprehensive review," Measurement, vol. 151, p. 107198, Feb. 2020, doi: 10.1016/j.measurement.2019.107198.

[23] I. Khan, I. Usman, T. Usman, G. U. Rehman, and A. U. Rehman, "Intelligent churn prediction for telecommunication industry," International Journal of Innovation and Applied Studies, vol. 4, no. 1, pp. 165–170, 2013.

[24] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk," IEEE Access, vol. 7, pp. 129551–129583, 2019, doi: 10.1109/ACCESS.2019.2932609.

[25] F. A. Majid and N. M. Shamsudin, "Identifying Factors Affecting Acceptance of Virtual Reality in Classrooms Based on Technology Acceptance Model (TAM)," Asian Journal of University Education, vol. 15, no. 2, pp. 51–60, Dec. 2019.

[26] H. Shaikh, M. S. Khan, Z. A. Mahar, M. Anwar, A. Raza, and A. Shah, "A Conceptual Framework for Determining Acceptance of Internet of Things (IoT) in Higher Education Institutions of Pakistan," in 2019 International Conference on Information Science and Communication Technology (ICISCT), Mar. 2019, pp. 1–5, doi: 10.1109/CISCT.2019.8777431.

[27] H. Rajab and T. Cinkelr, "IoT based Smart Cities," in 2018 International Symposium on Networks, Computers and Communications (ISNCC), Jun. 2018, pp. 1–4, doi: 10.1109/ISNCC.2018.8530997.

[28] R. Bukhsh, N. Javaid, M. I. Khan, Z. A. Khan, and I. Usman, "Cost efficient hybrid techniques for DSM in smart homes," International Journal of Ad Hoc and Ubiquitous Computing, vol. 33, no. 2, pp. 90–108, Jan. 2020, doi: 10.1504/IJAHUC.2020.105462.

[29] B. Caddy, N. Pino, and H. S. L. 3 days ago, "The best smart speakers 2020: which one should you buy?," TechRadar Middle East. https://www.techradar.com/news/best-smart-speakers (accessed Sep. 28, 2020).

[30] D. Gershgorn, "The Apple Watch Is the New Starter Phone," Medium, Sep. 15, 2020. https://onezero.medium.com/the-apple-watch-is-the-new-starter-phone-4eb74ed61e0b (accessed Sep. 16, 2020).

[31] S. Liesman, "America loves its Apple. Poll finds that the average household owns more than two Apple products," CNBC, Oct. 10, 2017. https://www.cnbc.com/2017/10/09/the-average-american-household-owns-more-than-two-apple-products.html (accessed Sep. 20, 2020).

[32] Yonghee Kim, Youngju Park, and Gwangsuk Song, "Interpretive Structural Modeling in the Adoption of IoT Services," KSII Transactions on Internet & Information Systems, vol. 13, no. 3, pp. 1184–1198, Mar. 2019, doi: 10.3837/tiis.2019.03.004.

[33] E. Shaikh and N. Mohammad, "Applications of Blockchain Technology for Smart Cities," in 2020 Fourth International Conference on Inventive Systems and Control (ICISC), Jan. 2020, pp. 186–191, doi: 10.1109/ICISC47916.2020.9171089.

[34] H. Tranter, "A survey on approaches to the protection of personal data gathered by IoT devices," PeerJ PrePrints; San Diego, Jul. 2018, doi: http://dx.doi.org.sdl.idm.oclc.org/10.7287/peerj.preprints.26473v2.