Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 22 No. 6 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v22i06.61533

SPECIAL FOCUS PAPER

An Internet of Things and Machine Learning Procedure to Rejuvenate Healthcare

Ahmad Tasnim Siddiqui[1], Ayma Fatima[2], Rasheedul Haque[3] (✉), Abdul Rahman Bin S Senathirajah[2,4,5], Sayeeduzzafar Qazi[6], Jessica Ong Hai Liaw[7]

[1]Horizon University College, Ajman, UAE

[2]INTI International University, Nilai, Malaysia

[3]MILA University, Nilai, Malaysia

[4]Shinawatra University, Bang Toei, Thailand

[5]Wekerle Business School, Budapest, Hungary

[6]University of Business and Technology, Jeddah, Saudi Arabia

[7]National Defence University, Kuala Lumpur, Malaysia

rasheedul.haque@mila.edu.my

ABSTRACT

Modern medicine's therapeutic applications unquestionably have a larger impact on people's daily lives than the Internet of Things (IoT). In this context, "things" might refer to a wide variety of tangible objects, including monitors for vital signs and other common metrics. Scales and other measuring tools are examples of such equipment. These devices connect to the web and transform information about your real-world setting into information about your digital one. They connect the real and virtual worlds so that they mediate between the two. Information gathered by these gadgets can be shared rapidly with other devices for analysis. This level of specificity illuminates the healthcare system and motivates new ideas to make better patient care without altering established procedures. Important factors of the healthcare business, such as recent developments, obstacles, and practical data, are expected to be considered by the research's conclusions. One way in which IoT has the potential to enhance medical treatment in underserved areas is in rural settings. The purpose of this specialist publication is to investigate how IoT could affect the delivery of healthcare and the function of computers in the industry.

KEYWORDS

healthcare, cloud, Internet of Things (IoT), data analytics, sustainable growth

1 INTRODUCTION

When compared to the entire population of the world, the number of devices that are linked to the internet is growing at a pace that is consistently faster than the population of humans. As a direct consequence of this, there is a significant need for interactions that are either entirely or in part automated. The level of development in technology has reached a stage where it is now feasible to capture data in real time, in addition to transferring and processing a significant quantity of digital content. The concept was established with the intention of enhancing one's degree of comfort while simultaneously reducing the amount of human interaction that is required in everyday living. Kevin Ashton of the MIT Auto-ID Centre [1] first came

Siddiqui, A. T., Fatima, A., Haque, R., Senathirajah, A. R. S., Qazi, S., Liaw, J. O. H. (2026). An Internet of Things and Machine Learning Procedure to Rejuvenate Healthcare. *International Journal of Online and Biomedical Engineering (iJOE)*, 22(6), pp. 106–123. https://doi.org/10.3991/ijoe.v22i06.61533

Article submitted 2026-03-14. Revision uploaded 2026-04-08. Final acceptance 2026-04-09.

up with the term "Internet of Things" (IoT) in order to conceptualize and put into action this notion (IoT). The word "things" needs to have a unique identity in order for them to be able to connect to the internet. One example of this is an IP address. IPv6 enters the picture due to the fact that the address space provided by the IPv4 protocol (2^{32}) is inadequate to assign identities to the vast majority of devices that are connected to the internet (address space 2^{128} is more than enough for address allocation). The IoT domain makes use of integrated features that are things-oriented (sensors), internet-oriented (middleware), and semantic-oriented in order to create a heterogeneous information system. These features are integrated because the Internet of Things domain aims to create a heterogeneous information system (knowledge). According to the ITU Internet Reports 2005 [2], the IoT is comprised of the following four components: radio frequency identification (RFID) technology, sensors, embedded intelligence, and nanotechnology.

Applications that are based on the IoT, provide a decision-making feature that operates in real time to generate an immediate response for end users. Applications need a framework that is capable of accommodating extremely large volumes of digital content, despite the fact that IoT devices are often very tiny, relatively cheap, and have limited storage capacity. In this scenario, customers would rather pay for the cost of utilizing a service than be concerned with the maintenance of resources. As a result, there has been a rise in the demand for renting space for storage and computation-intensive activities. In this scenario, it is necessary to give some consideration to the concept of a cloud model. The beginnings of this concept may be traced back to distributed computing, parallel computing, and grid computing [3]. IaaS, which stands for "Infrastructure as a Service," is a concept of providing computer and data storage on a leasing basis. This approach is also known as "cloud computing" [4]. In this form of service, rather than directly purchasing the expensive workstations, servers, and storage devices, the service provider contracts them out to a third party. The Platform-as-a-Service (PaaS) model of cloud computing provides customers with access to a platform that has all of the toolkits and resources required to construct applications and services. In order for users to access the software that is provided by Software-as-a-Service (SaaS), they need to be connected to the Internet. This is because users do not have to worry about installing, storing, or upgrading the program themselves (SaaS).

As a direct result of advancements in technology, the globe as a whole has seen a substantial amount of change in the most recent decades. One example of this category of applications is the use of the IoT in the field of medicine. According to [5], the IoT is composed of embedded systems that are put to use for the purpose of communicating with both the interior and the outside surroundings. According to the Internet Engineering Research Consortium (IERC) [6], the IoT is a worldwide wide-area infrastructure that is capable of self-governance. This infrastructure consisted mostly of certain standard protocols and numerous qualities that have intelligence and the integration of a large number of different networks; these were utilized for communication. The standard for the protocol requires the identification of a large number of features that are used in the process of communication [7]. Individuals are able to connect from any place and at any time, regardless of where they are located on the planet, thanks to the IoT. The proliferation of Internet-connected devices has seen a major uptick in recent years, thanks in large part to the advent of mobile computing devices such as smartphones, tablets, and smart televisions. These clever devices may be used in a wide range of contexts, including the medical sector, which is only one of several sectors that might benefit. According to the opinions of medical professionals, the use of IoT technology in the healthcare industry

has made great advancements and is more beneficial [8] in all aspects. The use of cloud storage space makes it possible to link the devices that make up the internet of things. In addition, the patient records may be viewed and monitored from a distant location, and in the case of an emergency, we can work together and share the pertinent information with one another. Additionally, we can monitor the progress of the patient from any point across the world by using an application that is downloaded into the patient's mobile phone.

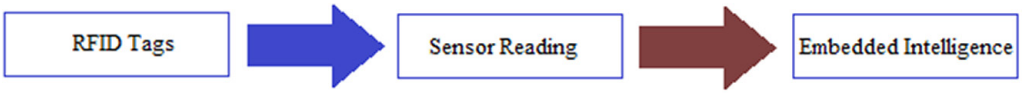

Fig. 1. Dimensions of IoT

Source: Created by the authors.

The concept of remote health was developed in an effort to provide high-quality medical support to patients located in remote areas, where there may not be easy access to hospitals, clinics, or medical specialists in the relevant field of medicine. This led to the conception of the term "remote health." It is conceivable to use remote health monitoring as a component of an assistance system for independent living that is suited for older individuals. In many cases, patients are more satisfied with the outcomes of their care after receiving remote health care as opposed to traditional medical therapy, and total expenditures are reduced [4]. One thought that exemplifies this concept well is the notion that people who opt to take part in assisted living programs have a greater chance of leading healthier and longer lives [9]. It is essential to keep a check on elderly people who are often left alone at home because of their vulnerability. There is a major shortage of individuals in today's society who are able to show compassion for other people and provide assistance to them when they are in need of it. Because of this, there was an increase in demand for healthcare services, but there were not enough personnel to meet that need. As a direct result of this, the demand could not be satisfied. In addition to making people's lives more challenging, frequent visits to patients' homes by healthcare personnel may push up the cost of providing care to a large degree. People's lives are also made more difficult by frequent visits.

During every stage of the creation of the overall concept, the needs of the users are carefully considered and accommodated wherever possible. A framework that is built on the IoT is an effective way for delivering healthcare services in remote places. This is due to the fact that the IoT is heterogeneous in nature and has the flexibility to accept "any" paradigm. Within the context of the remote health framework, information on an individual's state of health may be gleaned via the use of sensor networks or body area networks. The sensing data that have been gathered from the many different smart nodes are first filtered, and then they are pooled together. It is speculated that a 6LoWPAN gateway [10] or edge router would perform the function of middleware in order to circumvent the challenges that are presented by resource-constrained networks. The Internet is responsible for the flow of data of all different types and is able to create a virtual environment in which vast volumes of data may be managed. The goal of storing large volumes of data on the system of a third party is a common reason for using the cloud computing environment. Moving patient records and other types of health information onto the cloud offers several advantages to the organizations who are responsible for providing medical care. Therefore, in the context of remote healthcare, a security solution that is based on standard norms has to be addressed [11]. The application-specific requirements of industrialized countries are often capable of being met by security policies that

are developed in line with the healthcare standards that are already in place [12]. The great majority of people who live in poor countries are completely unaware of the dangers that they are up against. As a result of the absence of an access control strategy that is both comprehensive and effective, healthcare apps are susceptible to misuse of the resources and services they provide. The creation of a generic access control model is an essential need for ensuring the safety of a resource or service, and it should be one of your top priorities.

Only machine-to-machine (M2M) communication isn't always practicable for applications like healthcare that have to deal with scenarios that need human engagement. Examples of such scenarios include patient monitoring and medication administration. The vast majority of IoT solutions that are on the market now are designed to work in completely automated environments. There is no infrastructure that is both universally applicable and capable of meeting the criteria of a significant number of applications that are utilized in real life [13]. There is an urgent need for a standardized approach to the construction of an IoT-based framework that is flexible to the functions that are brought about by different sorts of application-specific conditions. This requirement must be met as soon as possible. If a real-world application, such as healthcare, can be considered a case study, then it will be much simpler to illustrate both the relevance of and the applicability of a framework that is built on the IoT. A framework of this sort may, however, become unstable at some time in the future as a result of the availability of a broad range of vulnerabilities in its security. According to the findings of the research on security, the steps of verifying one's identity and exercising control over access are two of the most important components.

2 LITERATURE REVIEW

The overwhelming majority of the commercial frameworks that are now on the market are unable to meet the essential business requirements (in terms of both cost and technology) of remote applications in developing countries. During the past few years, there has been an increase in the number of studies and commercial projects that use the IoT paradigm in order to capture data in an omnipresent manner, to analyze data in a timely manner, and to distribute resources in the area of remote application. According to a review of the relevant literature [14], there is no remote application framework within the IoT paradigm that is based on the general needs and that can be reused after being fine-tuned in accordance with the requirements of individual applications. This is the conclusion that can be drawn from the fact that there is no framework for remote applications that is based on the general needs. Existing frameworks for IoT are notoriously difficult to adapt in general due to the high dependencies that they have on a large number of other components. There is a possibility that IoT-based frameworks that are built on the foundation of functionality-specific partitioning would have problems. When the requirements for an application are modified, it is required to make adjustments to the different kinds of layers as well as to rebuild the basic architecture of the program. The IoT paradigm, which is founded on M2M communication, is nearing its limitations as a consequence of the absence of a clear description of varied interactions among heterogeneous entities [15]. M2M communication is the foundation of the IoT paradigm. This is especially true for predicaments that need participation from actual people. The traditional workflow management system is unable to handle the complicated operations required by the IoT paradigm. The vast majority of studies that are pertinent to process net analysis are based on web service modeling. This modeling will need to be built upon in order to support the IoT paradigm. In a similar vein, IoT services are represented using a range of alternative

high-level Petri net models, which may enhance the complexity in some scenarios [16]. The vast majority of these attempts entirely ignore the need to include security as an integral part when building the framework [14]. In poor countries, difficulties arise in the transmission of information between the different kinds of devices as a result of a lack of availability or the high cost of communications standards for Internet of Things-linked devices (full automation through M2M interactions). Due to the lack of stable connectivity within the infrastructure of IoT, especially in rural India, it is not feasible to guarantee connection in India 24 hours a day, seven days a week. In fact, it is not even conceivable. Lack of awareness levels of IoT environment, in addition to its security and the exploitation of cloud storage [17], are some of the primary barriers to the effective deployment of IoT-based framework in actuality. In this part, we will provide an outline of the research gaps that have been identified about this subject. Frameworks that are already in existence for IoT are developed with a functionality-specific segmentation serving as their foundation. When the functional requirements of entities for an application are changed, this may be a challenging situation since the kinds of layers need to be modified, and the framework has to be rebuilt. Additionally, it has issues with scalability, which makes it difficult to keep up with the fluctuating requirements of consumers. The IoT [18] paradigm, which is based on M2M communication, is running into limitations due to the lack of standard infrastructure and explicit specification of various interactions among heterogeneous entities. This is particularly true for circumstances that call for the involvement of a person. The traditional workflow management system is unable to handle the complicated operations required by the IoT paradigm. The vast majority of remote services, in point of fact, are unable to tolerate failures during runtime or delays in response times [19]. These issues are often the result of flaws in the architecture of the system. The vast majority of studies that are pertinent to process net analysis are based on web service modeling. This modeling will need to be built upon in order to support the IoT paradigm. In a similar vein, IoT services are represented using a range of alternative high-level Petri-net models, which may enhance the complexity under certain conditions. The vast majority of these publications take absolutely no account of the fact that the modeling of services should always include security as an integral part of the process.

When using a keystroke-based (unit-modal) free pattern analysis, it can be particularly difficult to determine the exact number of enrolled patterns that are able to make a final choice for identity verification when the process is conducted in repeated mode. This is because the number of patterns that can do so is dependent on the specific keystrokes that are being analyzed [20]. Another important issue that has to be answered is how to combine patterns that have never been registered before in order to reduce the amount of administrative work that is required for the whole process. The selection of the appropriate monitoring mode (whether it should be continuous or periodic) and the evaluation of the appropriate interval length for periodic monitoring are two additional difficulties. Other tough challenges include the identification of the correct monitoring mode. It is not possible to establish the efficacy of the logic to protect the system framework from impostors during iterative user identity verification using only the standard metrics that are required in order to measure the correctness of the classification. This is because it is not possible to measure the correctness of the classification using only the standard metrics. In order to verify the identity of users based on a variety of input patterns from any stroke-based input device with varying types and sizes, another challenge is how to design a generic processing model that can be adapted to any context. This must be accomplished without increasing the processing time or the overhead.

In the context of remote health care, the most significant drawbacks of MAC are its high cost, its inability to activate dynamic access rights, and its reliance on

a central authority to determine which kinds of resources may be accessed and by whom. In addition, MAC requires a central authority to decide which kinds of resources may be accessed. In a similar line, some of the drawbacks of DAC [21] include an inability to govern the flow of information during run time, ignorance of the incorrect assignment of permissions, and a lack of scalability in instances involving remote health care. Neither the MAC nor the DAC is able to control access in the case of a crisis. As a consequence of this, the health conditions seen in more remote places will render these efforts ineffective. Although the most widely used role-based access model (RBAC) in healthcare has several advantages over traditional identity-based access control (DAC, MAC) [22], it still faces several challenges when it is deployed in the real world. Despite these challenges, RBAC has become the most widely used model for controlling access in healthcare [23]. In order to give patients therapy that is of sufficient quality, it is necessary to fulfill these requirements. RBAC is unable to detect whether a remote health resource is sensitive or not. It will not be effective if patient–doctor links are created on the basis of identity rather than role in order to avoid the assignment of any clinician to a patient who has certain symptoms [24]. When the system framework generates a high number of access requests all at once, it is hard for the framework to decide whether or not to provide access within a reasonable length of time. This is because the framework does not have enough information to make an informed decision. It makes it more difficult for the medical professionals to have timely access to the medical reports of their patients. The RBAC is unable to supervise the sequence in which surgeons perform procedures in order to give patients the correct treatment. The drawbacks of traditional RBAC are mitigated in attribute-based access control (ABAC), often referred to as [25]. This is because ABAC is used in the context of its use on the traditional Internet. However, since there is a lack of knowledge about all of the features, it is hard to describe the policy in advance. This makes it difficult to determine whether or not the option made about access control is the proper one. When there are more users and more characteristics in an ABAC system, the system will become more complicated and less adaptive as the number of users and characteristics increases. We have acknowledged that the purpose of our research is to develop a model for dynamic access control that takes into account a variety of perspectives. The first issue to take into consideration is the fact that traditional techniques of access control will not work very well in a remote health scenario [26]. Consider, as an additional point of interest, the fact that models of access control were designed particularly for fully automated IoT [27] environments that cannot be used for applications with minimal budgets, scenarios with limited resources, and the need for human connection.

3 VISION AND ARCHITECTURE

Since the IoT is still in the process of being developed, each researcher has their own unique perspective on it. In light of the many points of view presented in this study, three concepts have been presented [28]. The cohesiveness of the many concepts is made abundantly obvious in Figure 2.

- A vision centered on the Internet
- A vision centered on semantics
- A vision centered on things

Embedded systems and networking play a significant part in things-oriented vision. This is a key component. In general, we make use of sensors in order to sense

the various physicochemical properties of the surroundings or atmosphere. Take, for instance, RFID and NFC; in addition, we are able to make use of Wi-Fi technology, WiMAX technology, Bluetooth, and a variety of other wireless technology interfaces. The sensor, which is coupled to the gadgets that make up the IoT, is able to detect all of the factors that are present in its environment. In order to get up-to-the-minute information, this concept will be put into practice.

Internet-oriented vision: The concept that underpins Internet-oriented vision is to link various intelligent gadgets by means of the Internet. This gadget utilizes Internet protocol ID in order to interact with other devices via the Internet. This vision offers the integration of the Internet and the smart gadgets that are linked to it, as well as the smooth monitoring of the surrounding environment. There are a number of different protocols that are standard that are used to describe Internet-oriented services. The globalization of these protocols in order to provide support for any Internet services was the primary motivation behind this approach.

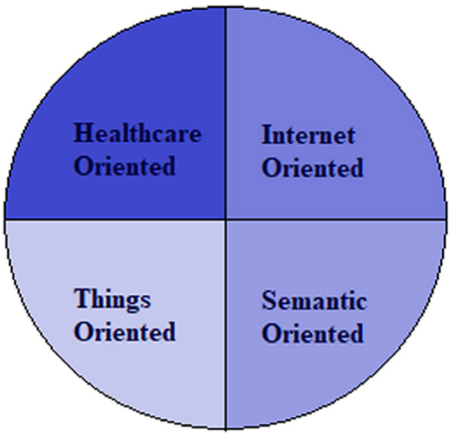

Fig. 2. Vision of IoT

Source: Created by the authors.

Vision oriented toward semantics: The primary goal of vision oriented toward semantics is to disentangle the raw input from any and all interpretations. This raw data that was taken from a variety of sensors contains information that is relevant. The semantic model has complete authority to choose relevant information from among the many possible interpretations. This approach makes use of semantic middleware, which, afterwards, serves as the foundation for semantic integrations in the physical world. Sensors are often responsible for the conversion of the physical quantities into their digital equivalents. Getting varied data is made easier by using a variety of sensors, such as those for temperature, pressure, and humidity, respectively. Actuators are the devices that are utilized for transforming digital signals into physical properties. This conversion may take place in a variety of different ways. Because of this, the combination of sensors and actuators may be employed as transceivers to send and receive the signals [29]. The whole architecture will be linked to the Internet so that the input and output operations may be controlled and monitored remotely. The diagrammatic representation of the detailed information may be seen in Figure 2. In human health data records, such as monitoring blood pressure, detecting blood glucose levels, and measuring heart rate, sensors and actuators are employed. Examples of these types of measurements include: The IoT can function in a more effective manner if it has access to these digitized health monitoring data. Researchers from a variety of backgrounds have conducted a number of studies on the topic of how well sensors may be utilized over the Internet [30].

4 HEALTHCARE TRENDS

The progression of technology, its benefits, and the many different functions that may be carried out by medical equipment are the primary factors that are considered when classifying healthcare [31]. Recent technology progress will make a future contribution to the expansion of healthcare in a variety of ways. These kinds of devices are used frequently in all electronic gadgets that are related in some way to smartphones [32]. For example, modern smartphones have health sensors that are kept inside as accessories, and these sensors can be used to monitor a person's health simply by having them worn, as is the case with smart wristwatches. This kind of equipment that supports m-health may be used to monitor both public and private health; in addition, it confers additional benefits on both the general population and members of the medical community [33]. The IoT may be broken down into the following categories depending to the functionalities involved [34]. i) It can be used to monitor and track. ii) It can be used for the recognition, encryption, and authentication of data. iii) A sensing and robotic system for the automatic collection of data. It is essential to provide an explanation of the potential uses of IoT as well as the emerging subjects in this area.

Access through Mobile Device: In the healthcare industry, as well as in hospitals, patient records are often kept in a digital format that is sometimes referred to as E-records or electronic health records. These records provide a number of advantages, including fast access to patient data and the ability for clinicians to observe patients. Through the use of a specialized application on a mobile device, such as a smartphone, the reliability of this system may be improved. Therefore, we may now replace the "word e-Health" with "m-Health," which refers to the practice of monitoring a patient and his data using an application on a mobile device [35].

Consultation Using a Virtual Approach: By utilizing remote connections, this method, shown in Figure 2, simplifies and streamlines processes for medical professionals and academics. Making connections distant for the purposes of performing surgery and giving lectures is now seeing a spike in popularity among medical professionals and academics [36]. The surgeons may now do their work from the comfort of their own homes with the assistance of medical robots and midwives (telemedicine). By using virtualization, it will be possible to make this system more stable while also cutting down on the amount of time needed for medical treatment. In a small number of nations, obtaining an appointment in a hospital might be an extremely difficult task.

Tracking and monitoring are two of the most important functions that these medical devices are responsible for doing. With the aid of other smart gadgets that include sensors, we will be able to monitor the patient's health if we use this particular equipment. Medical professionals can use the information obtained from these sensors to analyze the data and then treat the patient appropriately based on those results.

Patient observation through wireless: This is used in order to wirelessly observe a patient while he or she is at a faraway location. For this purpose, we make use of a transmitter and receiver that are linked between the patient and the doctor and are attached to both internal and exterior equipment. For instance, a wireless pacemaker can send information to the attending physician in the event of a medical emergency, such as a malfunction in the device, a change in blood pressure, or any other scenario. This information can then be used to manage, monitor, and administer treatment in the shortest amount of time possible. There are sensors included inside the gadget that collect data and send it to the careers so that continuous monitoring may take place.

The elderly may be monitored at home or at a hospital using this equipment, which was specifically designed for that purpose. For autonomous monitoring that does not need human interaction, this gadget comprises a smartphone equipped with a receiver

as well as a transmitter that is designed to be connected to the patient. This monitoring gadget constantly collects data from the patient and sends that data to a smartphone. The information is then sent from the smartphone to the person who is responsible for the patient's care. When the device detects an emergency, it immediately sends the data to nearby hospitals. As a result, it lowers the risk of complications during treatment as well as the cost of treatment itself because the necessary steps are taken to admit the patient as soon as possible. The data that is sent to the hospital will be utilized for post-analysis, which is performed with the assistance of real-time data that is easily accessible in the database. This analysis will take place after the data has been sent. With the use of IoT, a variety of sources can be searched in order to gather data related to patients. When this information is utilized, medical professionals are able to make significantly more informed decisions, which ultimately benefits the patient's overall health. In addition, IoT makes it possible to conduct a video consultation, which connects many physicians located in any part of the globe to respond to a medical emergency in a single minute. People in today's society place a greater emphasis on receiving treatment that is both quicker and more effective, as well as therapy that is more economical.

5 TASKS AND CHALLENGES

IoT is facing lots of challenges, just like other technologies do, such as social and ethical ones, getting permission from regulatory board, and promoting the market as well as technical flaws and challenges to overcome due to the fact that regulatory boards and the government are involved in all aspects of IoT activity; the protection of personal information is a primary issue. Therefore, the government as well as other sectors that are engaged are taking the required measures in promoting privacy and security in order to prevent the theft of data and the infiltration of others.

Interoperability: Interoperability is a significant difficulty since there is a vast deal of technology present practically everywhere, making it difficult to combine all of these technologies into a single system. Integrating all of those technologies presents a number of significant hurdles. Therefore, in order to accomplish the integration of all technologies with the internet of things, we need a protocol framework. However, since we are so far behind in developing integration standards, this presents a significant challenge and is of the utmost importance. Because of this restriction, it will be exceedingly difficult to make any additional progress toward improving interoperability.

Inadequate assistance from the government—It is critical that the government organizations and regulatory board provide support for the protection of individuals' privacy and security. They need to insist on a standard committee to organize and support devices connected to the internet of things as well as the purposes such devices have for the general population. This situation has to be rectified so that services related to the internet of things may be carried out in a more effective manner. Currently, there is insufficient assistance from government agencies and regulatory boards.

"Scalability" refers to a cloud network that is utilized by IoT to link or interconnect millions of people all over the globe. Because of this, a massive quantity of data has to be handled by sensors. Managing all of this information while also making IoT more efficient is one of its major challenges. In addition, this raw data has to be evaluated in an efficient manner in order to generate findings in real time for a few different types of emergency scenarios.

For the patient's protection and safety, IoT devices are linked to their cellphones and surgically implanted in various regions of their bodies. People who are using implanted devices in their bodies and who are uninformed of the negative influence of the device,

which may lead to some injury in the body, particularly if it is used by elderly people, are at the highest risk of this happening to them. This is the largest hazard.

Because the IoT relies on wireless communication, there is the potential for security breaches to take place, and this is the aspect that has to be improved upon. Individuals' privacy is another concern that must be addressed. It is required that the personal information of the patient as well as his health records be protected. Any compromise in the system's security, of any kind, will result in severe exploitation of the system.

We are in possession of the technology that is expanding at a rate that is far quicker than any other technology. However, there are still a few obstacles that stand in our way, such as the fact that the IoT has limited energy, memory, and processing capacity. When it comes to the design of an IoT-enabled device, this presents a significant difficulty.

6 METHODOLOGY

The IoT travel itinerary is shown in Figure 3. This demonstrates the progression of technology from 2000 to 2020.

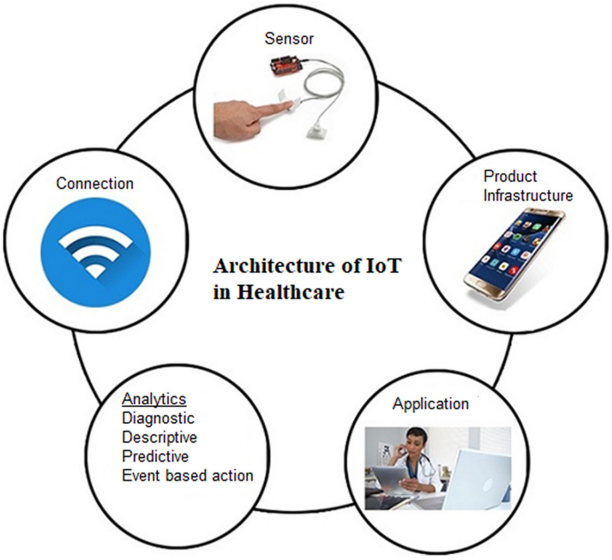

Fig. 3. Architecture of IoT in healthcare

Source: Created by the authors.

At this time, we have a desire for faster logistics, in which RFID tags play a significant role and contribute to the prevention of loss. The second adjustment will first focus on monitoring, food safety, and the administration of documents. Additionally, we refer to them as applications for vertical markets. After the year 2010, there was a significant improvement in IoT, which allowed individuals and all objects to be located anywhere on the globe. In order to do this, they depend on cloud computing and smartphone technology in addition to the sensors they utilized for monitoring and managing the data. Because of this, there was a significant shift in the technology, which resulted in the development of teleoperation and telemedicine. These fields allow users to monitor and operate items from a distant place, making them extremely helpful for medical facilities. By using telemedicine, medical professionals can monitor and regulate a patient's condition from almost any location in the universe. It is likely that by this time, data collected from sensors will be connected to the real world through IoT.

7 FUTURE HEALTHCARE SYSTEMS

Two experiments are conducted to assess the effectiveness of the proposed diabetes system. The first experiment is conducted on the data acquired by the diabetes application, while the second experiment uses the benchmark Pima Indian diabetes dataset. The diabetes application captures the PHR information of 240 individuals, 150 of whom have diabetes and 90 of whom do not.

Ingestible sensor: The next generation of medical technology will consist of ingestible sensors, which may be as simple as a tablet that is taken orally and passed through the intestines to monitor and send the necessary data to a centralized hub. The primary purpose of these tests is to determine whether or not the medication that we are now taking is effective. These gadgets do not need a battery or an antenna to function properly. After being ingested, it absorbs liquids from the stomach and initiates a series of chemical events in order to activate the sensor. This technology not only monitors but also evaluates things such as x-rays, biopsies, blood tests, blood sugar levels, and heart rates without the need for any kind of external physical inspection. These capsules are most helpful for those who regularly take medication, particularly for conditions that are considered chronic. As the sensors transmit data, the data will be linked up with the real world, and in an emergency, it will reach the relevant medical facilities or healthcare person. Figure 4 provides a visual representation of the complete system.

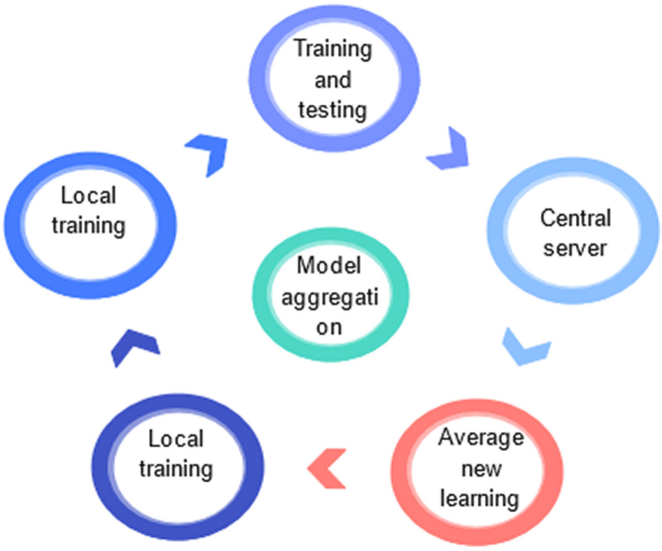

Fig. 4. IoT in federated healthcare

Source: Created by the authors.

Digital medicine: The digital version of medication is an improvement over the traditional method. Because the medication, rather than being cleared by a pill, will function as a tracking system, its moniker, "digital medicine," reflects this innovation. The patient takes a medication that continuously monitors the changes that are taking place inside the body and transmits those changes to either the outside environment or a centralized hub. At the hub, we are able to carry out all of the necessary observations and monitoring while the doctor keeps a close eye on everything. The patient will get a report detailing the changes that are taking place inside their own body, providing them with the ability to keep track of their condition in real time and making this method more effective.

Algorithm 1: Proposed Secured Transmission

call translate (claim expression, WFI) /
phase for identifying workflow instances call fragment (WFI) / WFI broken down into a sequence of tasks
do while (q is not empty) /
waiting queue q task = operator /
an operation operator being assigned to a task
Fix(source) = Si /
Set the source to the object's owner.
Fix(destination)= Sj/
destination set to object claimer/user call eval trust (Si, Sy) / trust evaluation phase
if 0.6 or trust value is less than 1.0, then trust level will be 1.
otherwise, if 0.1 ≤trust value ≤0.5 then,
trust level=2
otherwise, if trust value < 0.0 then,
trust level=3

7.1 A statistical investigation based on the case study

Mountaineers have been used in a demonstration to illustrate a point. It is of the utmost importance to keep an eye on those who participate in dangerous activities such as mountain climbing or adventuring since each year there are a great number of fatalities that occur all over the globe as a direct result of inadequate monitoring of mountain climbers. In this presentation, a system consisting of a monitoring band and a smartphone equipped with an application has been exhibited. The mountain climber will be equipped with a wristband, and the touring adviser or other authority responsible for arranging the event will have access to a smartphone. A wristband equipped with sensors will carry out continuous monitoring of the participants and will communicate with the participants' smartphones via an ad hoc protocol. Through the use of long-distance communication protocols, it is possible to conduct remote surveillance [37]. If the gadget detects any kind of aberrant functioning, it will sound an alert, and then appropriate measures may be done immediately. The device configuration and a snapshot of the application are shown in Figure 5.

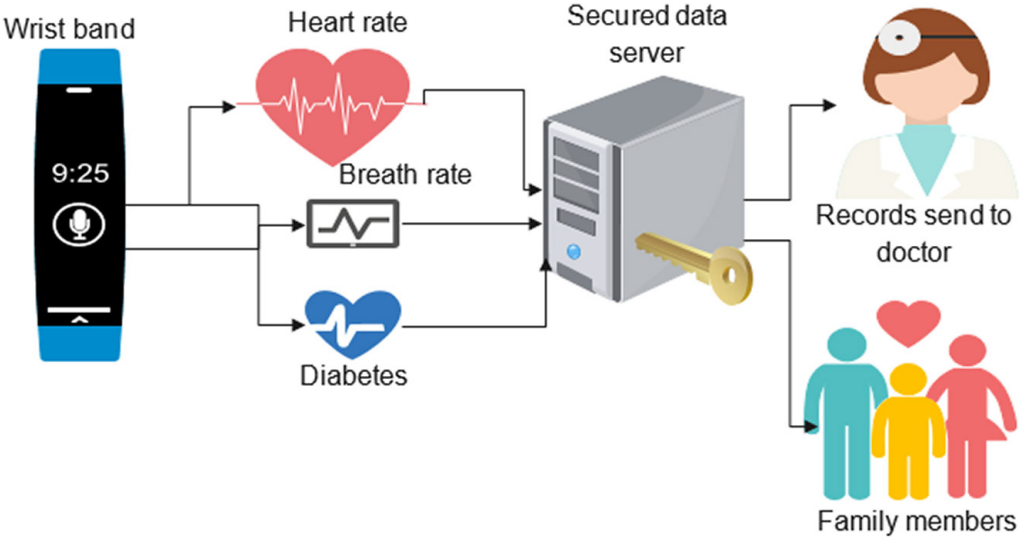

Fig. 5. Ingestible sensor network

Source: Created by the authors.

The measurement of the subject's heart rate with regard to the period of time is shown in Table 1. Additionally, Table 2 provide a comparison of the different communication protocols that are used for efficient communication over short and long distances, respectively.

Table 1. Illustration of heart rate vs. time period using sensors

S. No	Time Period	Heart Rate (bpm)
1	00:00	82
2	00:30	86
3	01:00	89
4	01:30	100
5	02:00	110
6	02:30	103
7	03:00	105
8	03:30	120
9	04:00	80
10	04:30	86
11	05:00	89
12	05:30	118
13	06:00	114
14	06:30	132
15	07:00	123
16	07:30	145

Source: Created by the authors.

7.2 Communication standards surveyed

Table 2. Comparison of short-range communication standards

	Bluetooth Low Energy	ZigBee(XBee Module)
Band of operation	2.4GHz	(2.402–2.480 GHz Utilized)
Topology	40 channels	79
Range	π/4 DQPSK	GFSK
Data rate	3 Mb/s	LE Coded PHY (S = 8): 125 Kb/s
Suitability for healthcare	≤100 mW (+20 dBm)	≤100 mW (+20 dBm)

Source: Created by the authors.

Personal healthcare records of individuals are frequently used in the literature for the diagnosis of various disorders. In addition, there are no known studies on the use of PHR in the context of diabetes diagnosis. The purpose of this approach is to aid in the proper identification of illnesses by physicians and doctors. Disease diagnosis

may be regarded as a more precise identification of the disease's symptoms. Once the symptoms are appropriately diagnosed, the condition is simple to treat. However, it is observed that these medical systems need significant processing power and resources. Medical systems are also reported to be computationally intensive [38].

Numerous scholars handle the problem of missing values in medical data by either detecting the missing value and deleting the corresponding data instances from the dataset or by using certain default techniques for filling the empty value, such as mean, median, neighbor, etc. However, neither approach produces excellent outcomes [39]. In addition, the presence of outliers in the data impaired the performance of the classifier. A small number of academics are also interested in the identification of outliers in medical datasets, although the topic has not yet been exhaustively investigated. This paper examines the effectiveness of PHR for diabetes diagnostic accuracy. Therefore, this paper provides a technique for monitoring diabetes patients utilizing their PHR. In addition, criteria are defined for the accurate diagnosis of diabetes. On the basis of PHR information gathered by a diabetic application, these guidelines are formulated [40].

This application is used to gather PHR information from various users and is also deployable in a mobile environment. Consequently, the purpose of this paper is to design a rule-based monitoring system for precise prediction and monitoring of diabetic illness [41].

8 CONCLUSION

The IoT is putting hitherto insurmountable obstacles, such as previously unavailable capabilities, into reach of almost everyone on the planet [42]. The IoT is seeing significant expansion in the field of healthcare, particularly in the areas of patient monitoring and medical recommendation, both of which can now be accomplished in a fraction of a second using an application [43]. This expansion is particularly notable in the areas of patient monitoring and medical recommendation. In today's environment, technology has made things easier for patients and their treating doctors by networking the whole world and delivering data in real time [44]. This is because technology can now provide more accurate information [45]. Because of these distinct benefits, we are able to provide the service in any region of the world in the shortest amount of time feasible. In spite of the challenges, developed and developing nations alike are striving toward the common objective of developing an advanced Internet of Things device that, if successful, would lead to improvements in medical treatment.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Ethical Approval: Formal ethical approval has been waived since this study adhered to the principles of the Declaration of Helsinki, following strict ethical standards. Participation was anonymous, confidential, and voluntary, with informed consent obtained from all participants. There were no biomarkers or tissue samples collected for analysis. Participants had the freedom to withdraw from the study at any point.

Data availability statement: Scopus database used. There is no data in hand.

Contribution: The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process: During the preparation of this work, the author(s)

used [ChatGBT—AI Chatbot] in order to [check grammar, spelling and references]. After using this tool/service, the author(s) reviewed and edited the content as needed and took full responsibility for the content of the published article.

9 REFERENCES

[1] Auto-ID Laboratory — Research Group. https://autoid.mit.edu/

[2] IERC – European Research Cluster on the Internet of Things, "Internet of Things – Pan European research and innovation vision," 2011.

[3] H. Jun-Wei, Y. Shouyi, L. Leibo, Z. Zhen, and W. Shaojun, "A crop monitoring system based on wireless sensor network," *Procedia Environmental Sciences*, vol. 11, pp. 558–565, 2011. https://doi.org/10.1016/j.proenv.2011.12.088

[4] A. Alam, M. Muqeem, and S. Ahmad, "Comprehensive review on clustering techniques and its application on high dimensional data," *International Journal of Computer Science & Network Security*, 2021.

[5] Gartner, Press release, 2013. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2014-12-15-gartner-says-the-internet-of-things-will-drive-device-and-user-relationship-requirements-in-20-percent-of-new-iam-implementations-by-2016

[6] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022. https://doi.org/10.1109/ACCESS.2021.3140091

[7] A. M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. DeVries, and J. Krapelse, "RFID application in healthcare – Scoping and identifying areas for RFID deployment in healthcare delivery," RAND, Europe, 2009.

[8] P. Pande and A. R. Padwalkar, "Internet of things–A future of internet: A survey," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 2, pp. 354–361, 2014.

[9] O. Vermesan and P. Friess (Eds.), "Internet of things: From research and innovation to market deployment," – *River Publishers*, 2014. http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

[10] C. Li, A. Raghunathan, and N. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *IEEE 13th International Conference on e-Health Networking, Applications and Services*, Columbia, MO, 2011, pp. 150–156. https://doi.org/10.1109/HEALTH.2011.6026732

[11] D. Christin, A. Reinhardt, P. Mogre, and R. Steinmed, "Wireless sensor networks and the Internet of Things: Selected challenges," in *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose Sensornede*, 2009, pp. 31–33. https://doi.org/10.1007/978-3-642-11917-0_3

[12] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021. https://doi.org/10.1007/s11045-020-00739-8

[13] Proteus, "Digital medicine," https://pure.eur.nl/en/publications/proteus-digital-health-healthcare-for-everyone-everywhere/

[14] HIPAA Privacy Rules: Information for Researchers. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html

[15] HL7 RBAC Model, "Version 3: Role-based access control healthcare permission catalog (RBAC)," [Online]. Available: https://confluence.hl7.org/download/attachments/104571102/HL7_V3_RBAC_R2_2010FEB.pdf?version=1&modificationDate=1614486392113&api=v2

[16] Indian Public Health Standards – Government of India. [Online]. Available: https://nhm.gov.in/index1.php?lang=1&level=1&sublinkid=284&lid=154

[17] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of Medical Systems*, vol. 43, no. 10, pp. 1–35, 2019. https://doi.org/10.1007/s10916-019-1445-8

[18] F. G. Mohammadi, F. Shenavarmasouleh, and H. R. Arabnia, "Applications of machine learning in healthcare and Internet of Things (IOT): A comprehensive review," *arXiv preprint arXiv:2202.02868*, 2022.

[19] S. H. Kim and W. Whitt, "Statistical analysis with Little's Law," *Oper. Res.*, vol. 61, no. 4, pp. 1030–1045, 2013. https://doi.org/10.1287/opre.2013.1193

[20] D. Ahirwar, P. K. Shukla, K. R. Bhatele, P. Shukla, and S. Goyal, "Intrusion detection and tolerance in next generation wireless network," in *Next Generation Wireless Network Security and Privacy*, IGI Global, 2015, pp. 313–335. https://doi.org/10.4018/978-1-4666-8687-8.ch011

[21] Y. Wang, G-Y. Du, and F-X. Sun, "A model for user authentication based on manner of keystroke and principal component analysis," in *Proceedings of International Conference on Machine Learning and Cybernetics*, 2006. https://doi.org/10.1109/ICMLC.2006.258999

[22] K. S. Balagani, V. V. A. Phoha, and S. Phoha, "On the discriminability of keystroke feature vectors used in fixed text keystroke authentication," *Pattern Recognition Letters*, vol. 32, no. 7, pp. 1070–1080, 2011. https://doi.org/10.1016/j.patrec.2011.02.014

[23] D. Gunetti, C. Picardi, M. Karnan, M. Akila, and N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," *Journal of Applied Soft Computing*, vol. 11, no. 2, pp. 1565–1573, 2011. https://doi.org/10.1016/j.asoc.2010.08.003

[24] M. Sathya *et al.*, "A novel, efficient, and secure anomaly detection technique using DWU-ODBN for IoT-enabled multimedia communication systems," *Wireless Communications and Mobile Computing*, 2021. https://doi.org/10.1155/2021/4989410

[25] A. Ahmed and I. Traore, "Biometric recognition based on free-text keystroke dynamics," *IEEE Transactions on Cybernetics*, vol. 44, no. 4, pp. 458–472, 2014. https://doi.org/10.1109/TCYB.2013.2257745

[26] T. Bhattasali, R. Chaki, K. Saeed, and N. Chaki, "Typing signature classification model for user identity verification," *Advanced Computing and Systems for Security*, Springer, vol. 666, 2018. https://doi.org/10.1007/978-981-10-8180-4_4

[27] B. Godi, S. Viswanadham, A. S. Muttipati, O. P. Samantray, and S. R. Gadiraju, "E-healthcare monitoring system using IoT with machine learning approaches," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 2020, pp. 1–5. https://doi.org/10.1109/ICCSEA49143.2020.9132937

[28] S. Giroux, R. Smolikova, and M. P. Wachowiak, "Keystroke based authentication by key press intervals as a complementary behavioral biometric systems," in *Proceedings of IEEE International Conference on Man and Cybernetics*, 2009. https://doi.org/10.1109/ICSMC.2009.5346319

[29] Z. Syed, S. Banerjee, and B. C. Leveraging, "Variations in event sequences in keystroke-dynamics authentication systems," in *Proceedings of IEEE International Symposium on High-Assurance Systems Engineering*, 2014. https://doi.org/10.1109/HASE.2014.11

[30] T. Shimshon, R. Moskovitch, L. Rokach, and Y. Elovici, "Clustering di-graphs for continuously verifying users according to their typing patterns," in *Proceedings of IEEE Convention of Electrical and Electronics Engineers in Israel*, 2010. https://doi.org/10.1109/EEEI.2010.5662182

[31] P. K. Shukla, L. Sharma, K. R. Bhatele, P. Sharma, and P. Shukla, "Design, architecture, and security issues in wireless sensor networks," in Next Generation Wireless Network Security and Privacy, IGI Global, 2015, pp. 211–237. https://doi.org/10.4018/978-1-4666-8687-8.ch007

[32] D. Gunetti and C. Picardi, "Keystroke analysis of free text," *ACM Transactions on Information and System Security*, vol. 8, no. 3, pp. 312–347, 2005. https://doi.org/10.1145/1085126.1085129

[33] S. Haykin, *Neural Networks: A Comprehensive Foundation*. Upper Saddle River, NJ: Prentice Hall PTR, 1998.

[34] Proteus, "Digital health feedback system," https://pure.eur.nl/en/publications/proteus-digital-health-healthcare-for-everyone-everywhere/

[35] C. Patel, A. K. Bashir, A. A. AlZubi, and R. Jhaveri, "EBAKE-SE: A novel ECC based authenticated key exchange between industrial IoT devices using secure element," *Digital Communications and Networks*, KeAI, vol. 9, no. 2, pp. 358–366, 2022. https://doi.org/10.1016/j.dcan.2022.11.001

[36] L. Adori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *ScienceDirect: Computer Networks*, vol. xx (Article in Press), pp. 1–19, 2010.

[37] R. Sivagurunathan *et al.*, "Equine-assisted learning and leadership transformation: An exploratory qualitative study of workplace behavior," *Front. Vet. Sci.*, vol. 12, no. 1700029, 2025. https://doi.org/10.3389/fvets.2025.1700029

[38] J. Alex *et al.*, "Multidimensional factors influencing consumers' purchase intention of green products: A company's strategy study," *Corporate & Business Strategy Review*, vol. 6, no. 3, pp. 328–336, 2025. https://doi.org/10.22495/cbsrv6i3siart9

[39] N. A. Aziz, S. Ahmed, R. Haque, S. Z. Qazi, and A. R. B. S. Senathirajah, "Deciphering international students' choices: Push-Pull dynamics and necessary condition analysis in Malaysian University selection," *International Journal of Knowledge Management*, vol. 21, no. 1, pp. 1–34, 2025. https://doi.org/10.4018/IJKM.372675

[40] B. Chawdhury, R. Haque, A. R. S. Senathirajah, M. I. Khalil, and S. Ahmed, "A structural path study modelling factors influencing social entrepreneurship intention: A Bangladeshi youth case study," *International Journal of Operations and Quantitative Management*, vol. 28, no. 2, pp. 418–440, 2022. https://doi.org/10.46970/2022.28.2.2

[41] S. Ahmed, R. Haque, A. R. S. Senathirajah, B. Chawdhury, and M. I. Khalil, "Examining the mediation effect of organisational response towards Covid-19 on employee satisfaction in SMEs," *International Journal of Operations and Quantitative Management*, vol. 28, no. 2, pp. 461–485, 2022. https://doi.org/10.46970/2022.28.2.4

[42] K. Kaur *et al.*, "Examining factors influencing fashion apparel purchases in omni-channel retailing: A post-Covid-19 study," *Transnational, Marketing Journal*, vol. 11, no. 1, pp. 44–58, 2023. https://doi.org/10.33182/tmj.v10i3.2182

[43] K. M. Umesh, A. R. S. Senathirajah, G. Connie, and R. Haque, "Examining factors influencing blockchain technology adoption in air pollution monitoring," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 4s, pp. 334–344, 2023. https://ijisae.org/index.php/IJISAE/article/view/2673

[44] A. A. Sumi *et al.*, "Investigating the function of religion and social capital in shaping sustainable social development," *Discover Sustainability*, vol. 6, p. 748, 2025. https://doi.org/10.1007/s43621-025-01622-x

[45] C. J. Ying *et al.*, "What drives IoT adoption? Insights from SMEs in manufacturing," *Journal of Cultural Analysis and Social Change*, vol. 10, no. 3, pp. 1012–1026, 2025. https://doi.org/10.64753/jcasc.v10i3.2542

10 AUTHORS

Dr. Ahmad Tasnim Siddiqui is a Senior Lecturer in the School of Computing, Horizon University College, Ajman, UAE. He has a keen interest in computing software, IoT, blockchain, cloud computer, data visualization, etc. (E-mail: tasnim5@yahoo.com, ahmad.siddiqui@hu.ac.ae).

Ayma Fatima is a master of science in data science student in the Faculty of Business and Communication at INTI International University, Nilai, Negeri Sembilan, Malaysia. With academic interests focused on research within the fields of computer science and software development studies (E-mail: i25037511@student.newinti.edu.my).

Dr. Rasheedul Haque, PhD, is working as an Associate Professor in the School of Management and Business (SOMB) at MILA University, Nilai, Malaysia. His research interests include entrepreneurship, quality service, hospitality & tourism, finance, and general management (E-mail: rasheedul.haque@mila.edu.my).

Dr. Abdul Rahman Bin S Senathirajah is a Professor affiliated under Faculty of Business and Communication at INTI International University, Nilai, Negeri Sembilan, Malaysia. His research interests include Quality Function Deployment (QFD), e-service quality, service quality, and smart card design and management (E-mail: arahman.senathirajah@newinti.edu.my).

Sayeeduzzafar Qazi, PhD, is a Professor and currently working as Chairperson of the Human Resources Management Department at the University of Business and Technology in Jeddah, Kingdom of Saudi Arabia. He was a member of the Academic Council of ICICI Prudential Life Insurance (Mumbai), as well as the Academic and Administrative Council of the Retailers Association of India (Mumbai) (E-mail: sayeed@ubt.edu.sa).

Dr. Jessica Ong Hai Liaw is an Associate Professor with a PhD in language psychology (psycholinguistics), communication, and linguistics from UPM (2010) and a BA in history, anthropology, and sociology from USM (2001). With certifications in teaching English studies, executive logistics and supply chain, and the Malaysia Commercial Certificate, she brings multidisciplinary expertise across psycholinguistics, communication, social integration, education, linguistics, and logistics. She also holds dual MBAs in Supply Chain & Logistics and Strategic Media & Communication (E-mail: jessica@upnm.edu.my).