Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

SMART AND SECURE IOT AND AI INTEGRATİON FRAMEWORK FOR HOSPITAL ENVİRONMENT

Mr. R. Valanarasu
Research Scholar
Bharathiar University
Coimbatore
Email id: valanarasu.r@gmail.com

Abstract: This paper presents a smart and secure framework for hospital environment using Internet of Things (IoT) and Artificial Intelligence (AI). This system overcomes the drawbacks of the current system of hospital information such as inflexible modes of networking, fixed point of information and so on. Factors such as basic network environment construction, application framework, logic structure, and data security are considered in detail. This work also helps in overcoming the existing problems of treatment, diagnosis, patient monitoring, and maintenance of hospital records in electronic format effectively. It presents a profound positive impact on the current methods followed in the hospital environment.

Keywords: Artificial Intelligence, Internet of Things, Healthcare, Data security, electronic medical records

1. Introduction

Electronic devices, actuators, sensors and software collectively forms a network that can actively communicate with each other. This network is termed as Internet of Things (IoT). Large volume of data can be generated by the networks, sensors and users that assists in gaining knowledge and developing applications with the help of Artificial Intelligence (AI) approaches. The combination of AI and IoT facilitates the advancement of public safety, education, healthcare, energy, transportation, and various such domains offering valuable services.

IoT in smart health care focuses on emergency services, smart computing, sensors, security, remote monitoring, and lab on chip, wearable devices, big data and connectivity. The security requirements of a smart hospital environment includes availability of services, data confidentiality, integrity, location privacy, data freshness, authentication, self-healing, identity threats, data eavesdropping, data privacy, resiliency, access control and unique identification.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

IoT systems also allows monitoring the health facts and the patient 24/7. Internet and other machines can be used for uninterrupted and remote monitoring of the health state of the patient. It also allows detection of critical illness at the right time and take suitable actions. Collection of health records, generation of statistical information pertaining to the health condition can be performed by IoT based machines. The processing of voluminous data can take place in an error free and quick manner [7].

Traditional hospital management systems contains problems like work overload for doctors and nurses, frustrating long lines, loads of paperwork, and so on. Integration of IoT to hospital environment can avoid all these drawbacks and replace the voluminous paperwork with a centralized and automated database. Remote monitoring of patients is also made possible. There are several technological obstacles, peculiarities and difficulties in implementation of this system. Technology is driven towards chatty hospital beds, fitbits and emergency drones. This paper proposes a novel system for integration of IoT and AI for a smart and secure framework.

2. Existing work

Jaisree et al [3] proposed a system for assisting the monitor of saline bottle level in hospital environment. In case of human negligence, improper monitoring may lead to demise of the patient. Due to the mismatch in the pressure between the empty saline bottle and the blood flow in the patient's body, there may be a mishap of blood flowing outward into the bottle. Continuous monitoring of the level and control can prevent such issues. Figure 1 represents Sample security attack in insulin supply monitor [4]. Active and passive attack models are also represented in the image.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

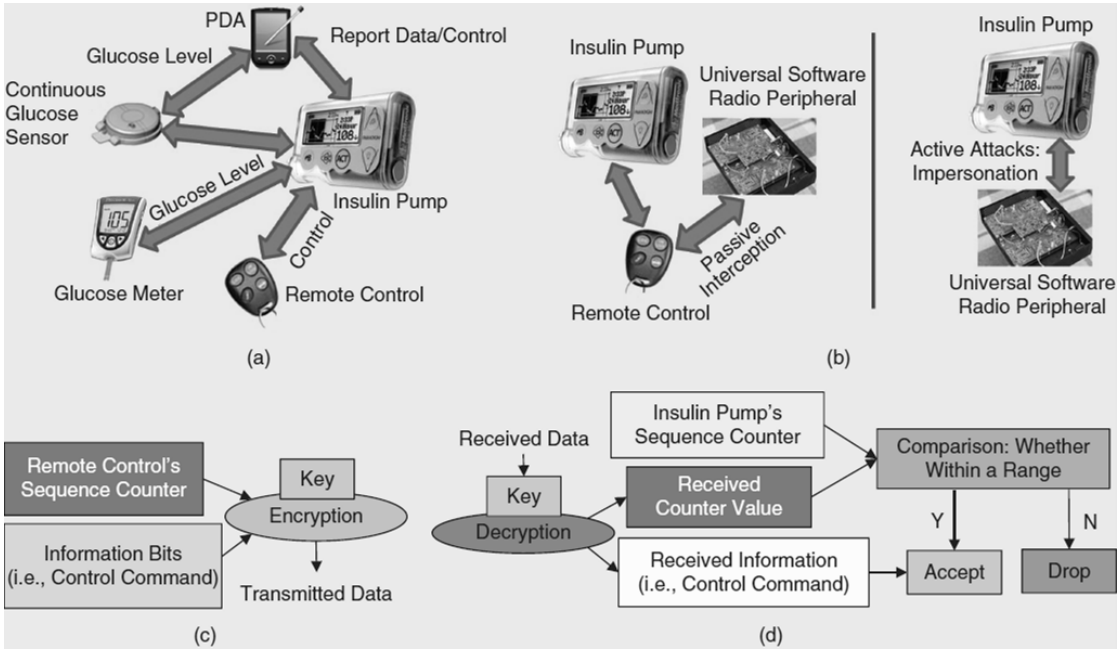

Figure 1: Sample security attack examples: (a) Insulin supply model; (b) active and passive security threats; (c) Remote controller with rolling-code encoding; (d) insulin pump with rolling-code decoding [4]

Dimiter V. Dimitrov [5] performed an extensive review of the application of big data and medical IoT in healthcare industry. The author proposed that communication of data gathered by the sensors is a major issue in IoT devices. This is because the different manufacturers have different protocols which does not allow the sensors to communicate with each other. Inflexible tendencies to store all the collected information, privacy concern, and fragmented software environment may cause data to be stagnated and inaccessible unable to deliver the complete utilization of the IoT system.

Seungjin Kang et al [6] performed a survey on the services that required IoT in hospital environment and analysed their demand. The services were categorized under three main domains namely patient safety improvement, work efficiency improvement and medical environment improvement. Pressure ulcer monitoring and management and fall system are the safety services; medical staff location tracking, real-time patient location tracking, medical monitoring, vital sign measurement device interface, rehabilitation management, hand disinfection system to prevent bacterial infection, smart patient transportation, continuous vital sign monitoring, and smart infusion pump are the systems to improve the work efficiency; smart wireless lighting, real-time asset tracking, ward instruments/equipment condition monitoring, and staff environment monitoring are the medical environment improvement services. Of all these services, it was identified that vital sign device interface system had the highest demand.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

Knickerbocker et al [8] applied heterogeneous integration to IoT, AI, algorithms, electronics, diagnosis and innovation in healthcare applications. The helps in improving the quality of life and offer chronic disease guidance. Vivek Agrawal et al [9] proposed privacy and security mechanisms like encryption, secure routing, secure authentication, freshness protection, and regulation and laws for wireless sensor networks used in healthcare. The authors also performed an analysis regarding security threats and offered its corresponding requirements and solutions.

Arun Iyengar et al [10] discussed about protected health information (PHI) and data security in healthcare informatics. Identification of ways to protect systems, processes and data in healthcare computing systems from various sources of attacks has been deliberated. The major reason for attacks is narrowed down to lack of proper encryption schemes and related key management. As a solution to this issue, homomorphic encryption is introduced. Privacy leakage may occur during verification of integrity if proper security and cryptographic actions are not taken. Information leakage may happen if a medical record that has multiple parts is accessed with a single digital signature for the complete record.

Ali Hassan et al [11] regulated transfer of data between entities in different devices efficiently and accurately using Product Lifecycle Management (PLM) and IoMT integration. Managing resource energy and battery lifecycle in small wearable electronics is done by joint energy harvesting and duty-cycle optimization-based (JEHDO) algorithm and battery recovery-based algorithm (BRA). Wolfgang Leister et al [12] developed a solution for context-aware adaptive security based on evaluation and authentication in e-health based IoT. The authors also developed a biomedical sensor based chronic disease analysis in home scenario and created a storyline for the patient.

Nawaf Alharbe et al [13] proposes a combination of IoT, Radio Frequency Identification (RFID) and Zigbee technologies in healthcare setting. Efficient management of location and tracking of objects is made possible by these technologies. It helps to detect and locate the staffs, assets, documents and patients with tags in the hospital environment. Ying Ma et al [14] performed an analysis on IoT based smart systems. The authors provided an overview of the benefits of IoT in smart healthcare where the patients can access their own medical records using internet via mobile applications and receive alerts for healthcare services.

Tathagata Adhikary et al [15] implemented an analysis of applications of IoT in healthcare. IoT is a lucrative choice for improvement of lifestyle and economy of the society. Ease of services, efficient resource handling, reduced manual error, better patient outcome, early diagnosis and patient engagement are the major benefits of IoT in healthcare. Rushabh Shah et al [16] performed an in-depth survey of AI and IoT in healthcare. Analysis is done based on the type of application, connectivity, treatment, sensor network and patient care.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

Mansour Naser Alraja et al [18] proposed a theoretical framework for risk perception using IoT and recommended enhancement of complexity of confidentiality and safety in IoT devices.

3. Proposed Work

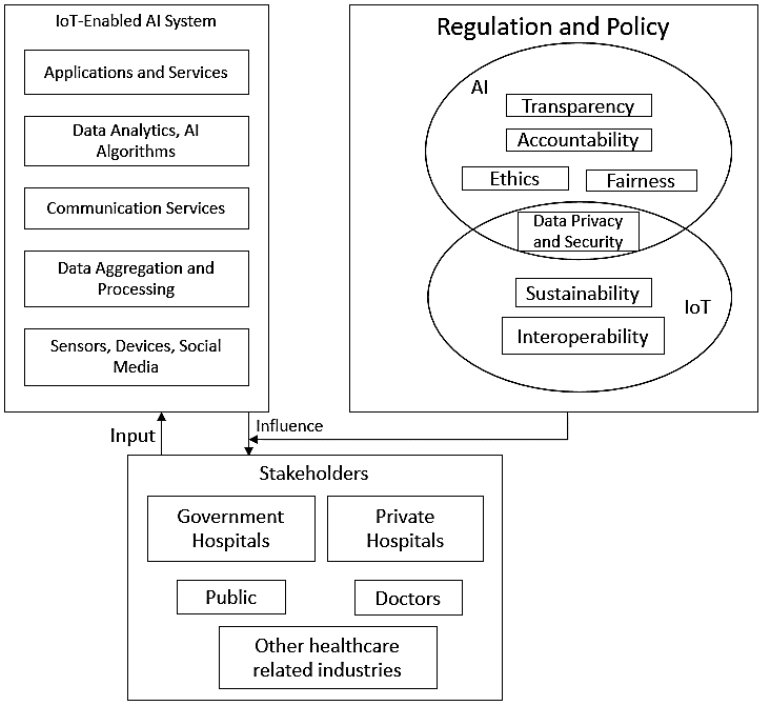

Figure 2: Block diagram representing the healthcare environment

The key factors to be considered in healthcare environment includes:

Security requirements: confidentiality, integrity, authentication, availability, data freshness, non-repudiation, authorization, self-healing.

Security Challenges: Computational limitations, memory limitations, energy limitations, mobility, scalability, communications media, and multiplicity of devices, dynamic network topology, multi-protocol network, dynamic security updates, and tamper-resistant packages.

Possibility of attacks:

Based on information disruptions – interruption, interception, modification, fabrication, and replay.

Based on host properties- user compromise, hardware compromise, and software compromise.

Based on network properties- standard protocol compromise, and network protocol stack attack.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

IoT based healthcare technologies: Cloud computing, grid computing, big data, networks, ambient intelligence, augmented reality, and wearable devices.

Open Issues: standardization, IoT healthcare platforms, cost analysis, application development process, technology transition, low-power protocol, network type, scalability, continuous monitoring, new diseases and disorders, identification, business model, and Quality of service.

Data protection: resource efficient security, physical security, secure routing, data transparency, IoT big data handling security; mobility, edge analytics, and ecological impact.

The proposed system works on basic network environment construction, application framework, logic structure, and data security. This work also helps in overcoming the existing problems of treatment, diagnosis, patient monitoring, and maintenance of hospital records in electronic format effectively. Figure 1 represents the architecture of this system. The IoT enabled AI system consists of an application and services layer that includes management applications and decision and hospital information application. The data like financial management, medical management, material and equipment management, drug management, physical therapy management, pathology, radiology, examination, and outpatient management information is stored in this layer.

Security is offered to the system by the regulation and policy layer that focuses mainly on the underlying structure's trust components such as safety, security, privacy, resilience, reliability, availability, sustainability, dependability and trustworthiness. This approach facilitates effective engagement of contractual arrangements, legislation, standards and ethics. Security-by design practices, network prescribed policy, authorization, authentication and security analytics are some principle security components taken into consideration.

4. Result and Analysis

This paper assisted the successful design of smart hospital using IoT and AI and integrating it with security features in the framework. We use a multifaceted system in which IoT is used for the integration of networking elements, displays, actuators, sensors, and other hospital devices and equipment. This contributes to the major trends in the IoT based hospital industry that works on wearable devices, surgical robots, and other recent technology devices.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

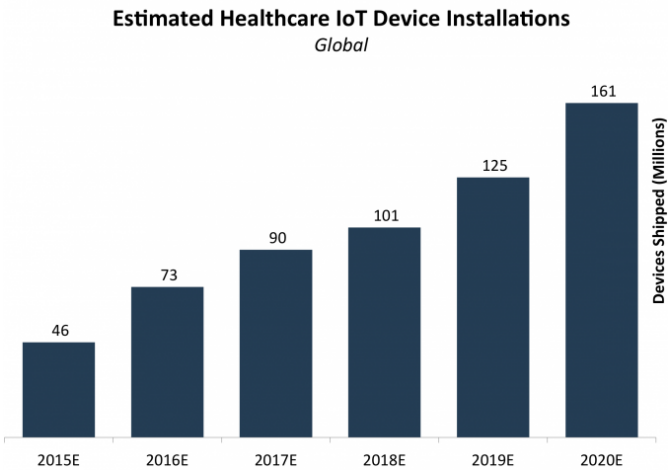

Figure 3: Estimated healthcare IoT Device Installations based on predictions from Business Insider.

5. Conclusion and Future Scope

There is a continuous increase in challenges and opportunities in IoT applications. IoT can also address fitness management, private health, chronic disease supervision, elderly care and paediatric care. We develop a novel system that offers secure integration of a smart hospital environment with the help of IoT and AI. The safety issues, privacy, adoption barriers and gaps of the existing smart systems are addressed. Future scope of this paper would be to work on reals settings and to perform large-scale testing of the model. It is also essential to investigate the adoption challenges, interoperability, and cultural, social, economic, and technical environment for implementation.

References

[1] Kankanhalli, Atreyi, Yannis Charalabidis, and Sehl Mellouli. "IoT and AI for smart government: A research agenda." (2019): 304-309.

[2] Islam, SM Riazul, Daehan Kwak, MD Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. "The internet of things for health care: a comprehensive survey." IEEE Access 3 (2015): 678-708.

[3] Jaisree, K., J. Sharmila, J. Jeevitha, and K. Chandrakala. "Smart hospitals using internet of things (iot)." *International Research Journal of Engineering and Technology (IRJET)* 3, no. 3 (2016): 1735-1737.

[4] Sundaravadivel, Prabha, Elias Kougianos, Saraju P. Mohanty, and Madhavi K. Ganapathiraju. "Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health." IEEE Consumer Electronics Magazine 7, no. 1 (2017): 18-28.

ISSN: 2582-1369 (online)

Journal of ISMAC (2019)
Vol.01/ No. 03
Pages: 172-179
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2019.3.004

[5] Dimitrov, Dimiter V. "Medical internet of things and big data in healthcare." Healthcare informatics research 22, no. 3 (2016): 156-163.

[6] Kang, Seungjin, Hyunyoung Baek, Eunja Jung, Hee Hwang, and Sooyoung Yoo. "Survey on the demand for adoption of Internet of Things (IoT)-based services in hospitals: Investigation of nurses' perception in a tertiary university hospital." Applied Nursing Research 47 (2019): 18-23.

[7] Darshan, K. R., and K. R. Anandakumar. "A comprehensive review on usage of Internet of Things (IoT) in healthcare system." In 2015 International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT), pp. 132-136. IEEE, 2015.

[8] Knickerbocker, John, R. Budd, B. Dang, Q. Chen, E. Colgan, L. W. Hung, S. Kumar et al. "Heterogeneous integration technology demonstrations for future healthcare, IoT, and AI computing solutions." In 2018 IEEE 68th Electronic Components and Technology Conference (ECTC), pp. 1519-1528. IEEE, 2018.

[9] Agrawal, Vivek. "Security and privacy issues in wireless sensor networks for healthcare." In International Internet of Things Summit, pp. 223-228. Springer, Cham, 2014.

[10] Iyengar, Arun, Ashish Kundu, and George Pallis. "Healthcare informatics and privacy." IEEE Internet Computing 22, no. 2 (2018): 29-31.

[11] Sodhro, Ali Hassan, Sandeep Pirbhulal, and Arun Kumar Sangaiah. "Convergence of IoT and product lifecycle management in medical health care." Future Generation Computer Systems 86 (2018): 380-391.

[12] Leister, Wolfgang, Mohamed Hamdi, H. Abie, and S. Poslad. "An evaluation framework for adaptive security for the iot in ehealth." International Journal on Advances (2014).

[13] Alharbe, Nawaf, Anthony S. Atkins, and Akbar Sheikh Akbari. "Application of ZigBee and RFID Technologies in Healthcare in Conjunction with the Internet of Things." In Proceedings of International Conference on Advances in Mobile Computing & Multimedia, p. 191. ACM, 2013.

[14] Ma, Ying, Kang Ping, Chen Wu, Long Chen, Hui Shi, and Dazhi Chong. "Artificial Intelligence powered Internet of Things and smart public service." Library Hi Tech (2019).

[15] Adhikary, Tathagata, Amrita Deb Jana, Arindam Chakrabarty, and Saikat Kumar Jana. "The Internet of Things (IoT) Augmentation in Healthcare: An Application Analytics." In International Conference on Intelligent Computing and Communication Technologies, pp. 576-583. Springer, Singapore, 2019.

[16] Shah, Rushabh, and Alina Chircu. "IOT AND AI IN HEALTHCARE: A SYSTEMATIC LITERATURE REVIEW." Issues in Information Systems 19, no. 3 (2018).

[17] Alraja, Mansour Naser, Murtaza M. Junaid Farooque, and Basel Khashab. "The Effect of Security, Privacy, Familiarity and Trust on Users' Attitudes Towards the Use of IoT-based Healthcare: The Mediation Role of RiskPerception." IEEE Access (2019).

ISSN: 2582-1369 (online)