International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-8)

Research Article | **August 2017**

Implementing Internet of Things in a Remote Patient Medical Monitoring System

Ifeoma V. Ngonadi
Dept. of General Studies (Maths& Computer Science Unit)
Petroleum Training Institute Effurun, Nigeria.

Abstract:

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. Remote patient monitoring enables the monitoring of patients' vital signs outside the conventional clinical settings which may increase access to care and decrease healthcare delivery costs. This paper focuses on implementing internet of things in a remote patient medical monitoring system. This was achieved by writing two computer applications in java in which one simulates a mobile phone called the Intelligent Personal Digital Assistant (IPDA) which uses a data structure that includes age, smoking habits and alcohol intake to simulate readings for blood pressure, pulse rate and mean arterial pressure continuously every twenty five which it sends to the server. The second java application protects the patients' medical records as they travel through the networks by employing a symmetric key encryption algorithm which encrypts the patients' medical records as they are generated and can only be decrypted in the server only by authorized personnel. The result of this research work is the implementation of internet of things in a remote patient medical monitoring system where patients' vital signs are generated and transferred to the server continuously without human intervention.

Keywords: Remote Patient Monitoring, Intelligent Personal Digital Assistant, Encryption, Decryption, Internet of Things

I. INTRODUCTION

The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data[3][4][15].

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure,[16] creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention [33][1][29][21][28][18]. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities [10]. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020 [24].

"Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters,[22] automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring,[7] or field operation devices that assist firefighters in search and rescue operations [36]. Legal scholars suggest regarding "Things" as an "inextricable mixture of hardware, software, data and service" [25].

IoT is one of the platforms of today's Smart City, and Smart Energy Management Systems[34][11].

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids [8]. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses [6]. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well [17]. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT[30]. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

In the internet of things (IoT), devices gather and share information directly with each other and the cloud, making it possible to collect, record and analyze new data streams faster and more accurately. That suggests all sorts of interesting possibilities across a range of industries: cars that sense wear and tear and self-schedule maintenance or trains that dynamically calculate and report projected arrival times to waiting passengers.

In a remote patient medical monitoring system, it is pertinent to have the patients' medical records stored in the cloud for a more secured access. As a result, patients with chronic diseases may be less likely to develop complications, and acute complications may be diagnosed earlier than they would be otherwise. For example, patients suffering from cardiovascular diseases who are being treated with digitalis could be monitored around the clock to prevent drug intoxication. Arrhythmias that are randomly seen on an EKG could be easily detected and EKG data indicating heart hypoxemia could lead to faster detection of cardiac issues. The data collected may also enable a more preventive approach to healthcare by providing information for people to make healthier choices.
The internet of things (IoT) plays a significant role in remote medical monitoring where patients wear sensors that monitor their vital signs and send the readings to a server in the hospital through existing networks or the Internet.
In this research work, a java program was written which simulates a mobile phone that uses data structure consisting of age, smoking habits, alcohol intake to simulate readings for blood pressure and pulse rate and send the readings to an online server.

II. RELATED WORK

In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[15] and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks"[2].
As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems[36]. This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things (IoT).[13].
The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance,[32] able to report its inventory and whether newly loaded drinks were cold[14].Mark Weiser's seminar 1991 paper on ubiquitous computing, "The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT[20][35]. In 1994 Reza Raji described the concept in *IEEE Spectrum* as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories"[27]. Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999 [26].
According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020 [31].ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of things by 2020[23]. As per a 2014 survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems[9]) will have widespread and beneficial effects by 2025[19]. As such, it is clear that the IoT will consist of a very large number of devices being connected to the Internet[2]. In an active move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of things. The former British Chancellor of the ExchequerGeorge Osborne, posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances[5].The Internet of Things (IoT) offers great promise in the field of healthcare where its principles are being applied to improve access to care, increase the quality of care and most importantly reduce the cost of care.
As the technology for collecting, analyzing and transmitting data in the IoT continues to mature, more and more exciting new IoT driven healthcare applications and systems continue to emerge.
Wireless sensor-based systems are at work today, gathering patient medical data that was never before available for analysis and delivering care to people for whom care wasn't previously accessible. In these ways, IoT-driven systems are making it possible to radically reduce costs and improve health by increasing the availability and quality of care. The ability of devices to gather data on their own removes the limitations of human-entered data automatically obtaining the data doctors' need, at the time and in the way they need it. The automation reduces the risk of errors. Fewer errors can mean increased efficiency, lower costs and improvements in quality in just about any industry. But it's of particular interest/need in healthcare, where human error can literally be the difference between life and death. The IoT plays a significant role in a broad range of healthcare applications, from managing chronic diseases at one end of the spectrum to preventing disease at the other. Here are some examples of how its potential is already playing out:
Clinical care: Hospitalized patients whose physiological status requires close attention can be constantly monitored using IoT-driven, noninvasive monitoring. This type of solution employs sensors to collect comprehensive physiological information and uses gateways and the cloud to analyze and store the information and then send the analyzed data wirelessly to caregivers for further analysis and review. It reduces the process of having a health professional come by at regular intervals to check the patient's vital signs, instead providing a continuous automated flow of information. In this way, it simultaneously improves the quality of care through constant attention and lowers the cost of care by eliminating the need for a caregiver to actively engage in data collection and analysis.

Remote monitoring: There are people all over the world whose health may suffer because they don't have ready access to effective health monitoring. But small powerful wireless solutions connected through the IoT are now making it possible for monitoring to come to these patients instead and vice versa. These solutions can be used to securely capture patient health data from a variety of sensors, apply complex algorithms to analyze the data and then share it through wireless connectivity with medical professionals who can make appropriate health recommendations.

III. THE SYSTEM ARCHITECTURE

A. Applying Internet of things in Remote Patient Medical Monitoring System

The Internet of Things in remote medical monitoring is shown in figure 1 where the patients' medical records are simulated in the Intelligent Patient Digital Assistant (IPDA). These records are encrypted in the security model, sent through the hub to the cloud where they are stored. The doctors can access the cloud when there is need to check on any patient's data and proffer solutions. This is also illustrated with the block diagram in figure 2 where the blood pressure, the pulse rate and the mean arterial pressure are simulated, sent through the hub which is the gateway to the cloud where the results are stored for easy access and reference.

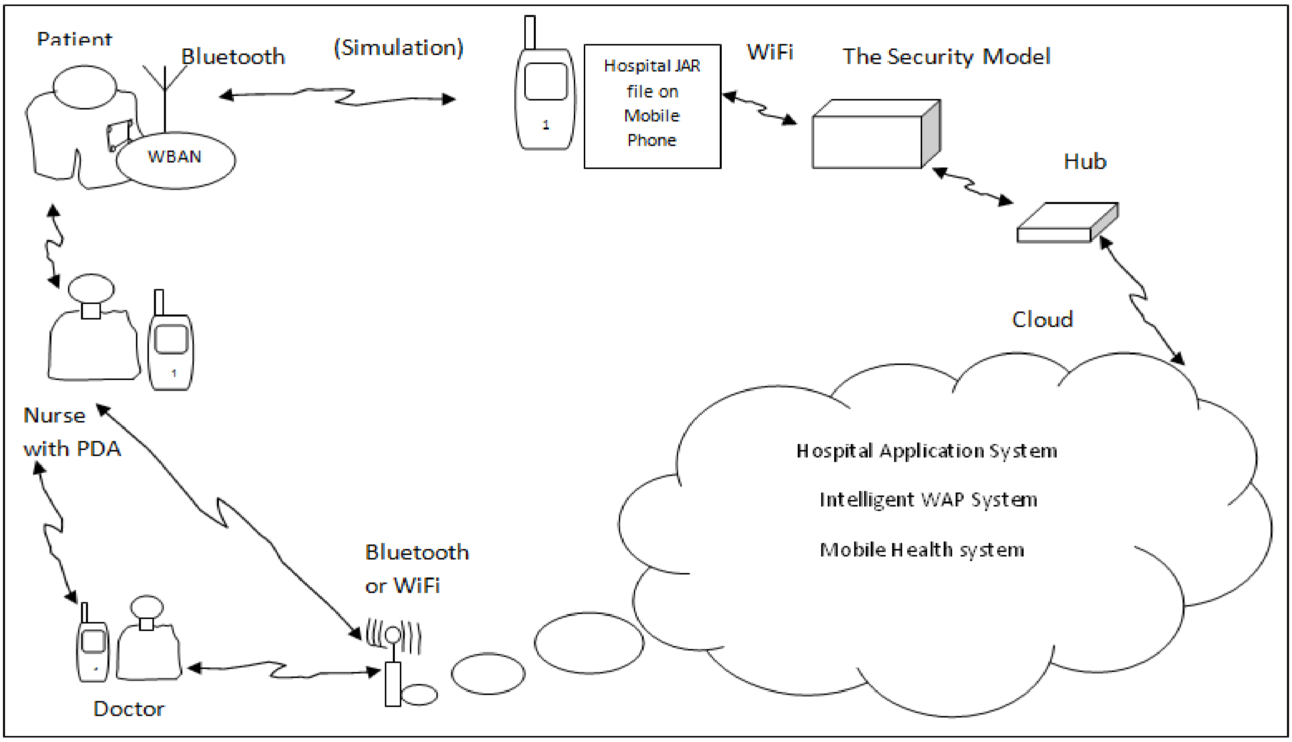


Fig. 1: Internet of things in Remote Medical Monitoring

The patients are fitted with sensors that monitor the blood pressure and the pulse rate which in this case are simulated by the Intelligent Patient Digital Assistant (IPDA) which is a simulated mobile phone responsible for simulating these results.

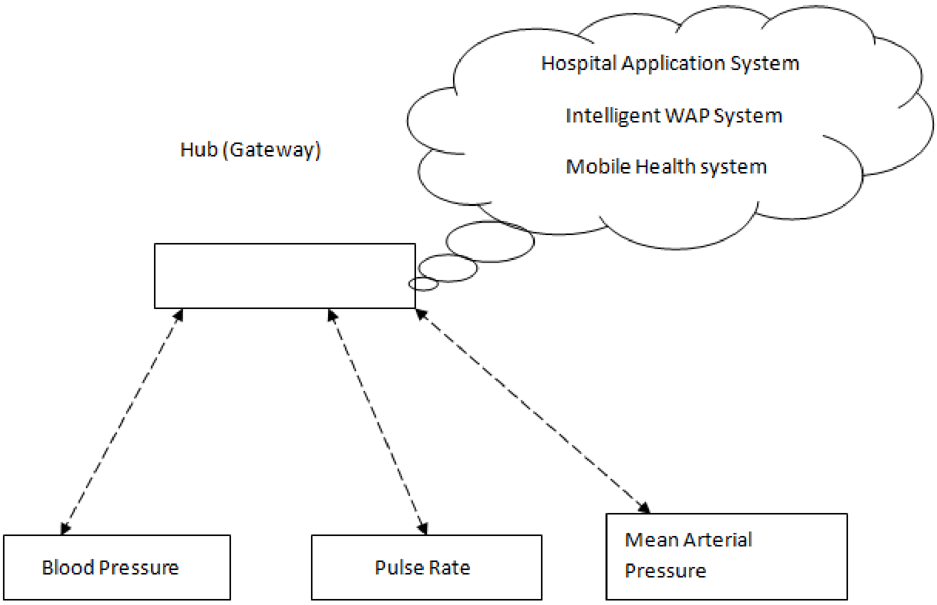


Figure 2: Block diagram of internet of things in remote medical monitoring

The simulated data from the patients are sent through the hub to the cloud. These patients' medical records are stored in the cloud and both the nurses and the doctors can access the cloud to check the patients' data and make informed and timely decisions.
The blood pressure, the pulse rate and the mean arterial pressure are simulated, generated and sent to the hub. The hub in turn captures patient data from a variety of sensors and securely stores it in the cloud, where it can be accessed by those engaged in the patients' care.
Gateways are the information hubs that collect sensor data, analyze it and then communicate it to the cloud via wide area network (WAN) technologies. Gateways can be designed for clinical or home settings, in the latter, they may be part of a larger connectivity resource that also manages energy, entertainment and other systems in the home.
Wireless networking removes the physical limitations on networking imposed by traditional wired solutions like ethernet and USB.

B. The Security Architecture
As the patients' medical records travel across networks, it is pertinent that they are protected against unauthorized access which might intercept the data along the way.
In view of this, the patients' medical records are encrypted as they travel across the networks, from the Intelligent Personal Digital Assistant to the server. This encryption is done by using the symmetric key encryption algorithm. In the encryption, the original text called the plaintext is encrypted using an encryption algorithm, to generate the encrypted text called the ciphertext that can only be read if decrypted.
The encryption scheme uses a pseudo-random encryption key generated by the algorithm. In the symmetric key scheme, the encryption and decryption keys are the same, thus communicating parties must have the same key before they can achieve secret communication.
The encrypted text which is the ciphertext is decrypted in the server by only authorized users using the decryption key which is the same key as the encrypted key.
In the security architecture, each patient is assigned a unique ID called PatientID (PID) which is generated using random number generation. The patientid generated is automatically encrypted. The patients' data are simulated with the Simulated Patient Data Software(SPDS) and sent to the Patient Data Acquisition Centre (PDAC) through wireless connection for consolidation and further transmission to the Central Hospital Monitoring System (CHMS) for processing and follow up by the medical care givers.

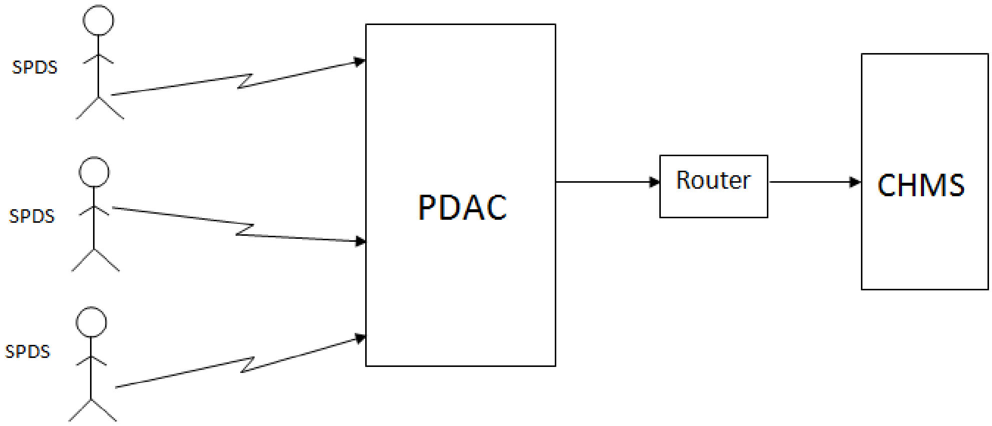


Fig. 3: The Security Architecture

Each patient is identified with a unique ID called Patient ID (PID). The PID identifies the origin of the data.
The transmission of patient medical data between the PDAC and the CHMS can be carried out by using a wireless router or the internet. The patients can be at home carrying out their normal duties while their physiological parameters are being monitored. Medical personnel can also monitor the patient data and alert the experts in emergency situations.
Wireless transmission can be insecure and prone to data loss. Therefore the security of the patient data is of utmost importance and this is ensured by encryption and decryption of the patient data as it travels from the PDAC to the CHMS.
Two physiological parameters namely Blood Pressure and Pulse Rate are monitored.
The two parameters (Blood Pressure and Pulse Rate)are generated for continuous monitoring of the patients and the encryption and decryption process was done by using the Symmetric Key Encryption Algorithm.

IV. RESULTS
The Intelligent Personal Digital Assistant simulates the blood pressure, the pulse pressure and the mean arterial pressure which it sends to the server. These readings are simulated continuosly every 25 secondsas long as the application remains active. The generated readings are kept in the mobile user log file.
Since the patients' data travel through networks, it is very important to protect them as they are prone to different types of attack such as eavesdropping, sending false values or replay of previous data. This was achieved with a second java program that encrypts the patients' records and safeguard them from unauthorized access. The records are decrypted in the server only by authorized personnel.

Fig. 4: The IPDA

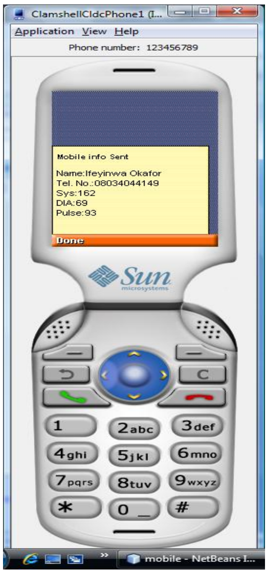
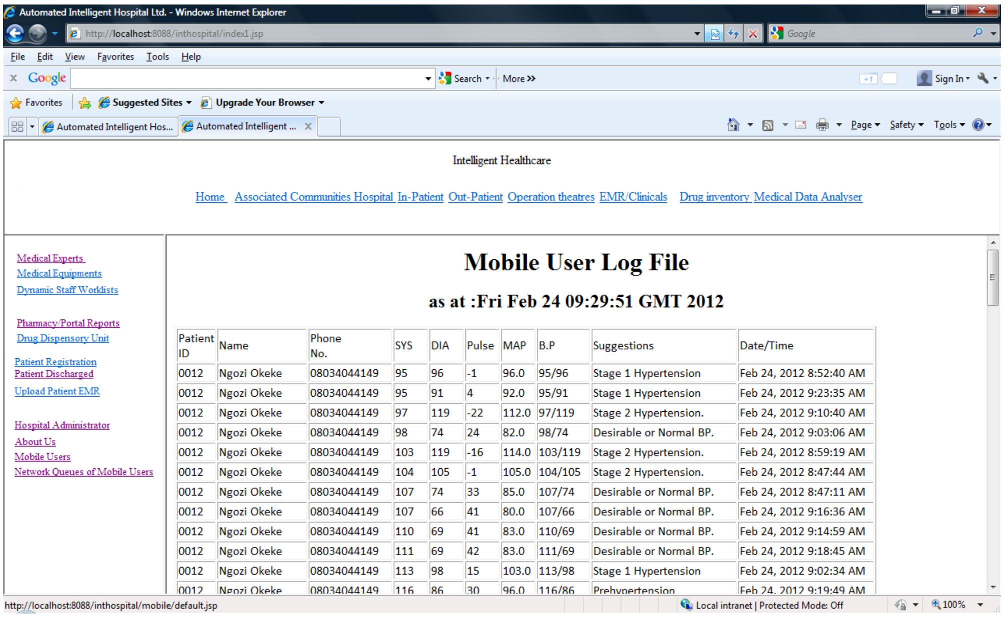


Fig. 5: Simulated reading for a patient



Mobile User Log File

as at :Fri Feb 24 09:29:51 GMT 2012

Patient ID	Name	Phone No.	SYS	DIA	Pulse	MAP	B.P	Suggestions	Date/Time
0012	Ngozi Okeke	08034044149	95	96	-1	96.0	95/96	Stage 1 Hypertension	Feb 24, 2012 8:52:40 AM
0012	Ngozi Okeke	08034044149	95	91	4	92.0	95/91	Stage 1 Hypertension	Feb 24, 2012 9:23:35 AM
0012	Ngozi Okeke	08034044149	97	119	-22	112.0	97/119	Stage 2 Hypertension.	Feb 24, 2012 9:10:40 AM
0012	Ngozi Okeke	08034044149	98	74	24	82.0	98/74	Desirable or Normal BP.	Feb 24, 2012 9:03:06 AM
0012	Ngozi Okeke	08034044149	103	119	-16	114.0	103/119	Stage 2 Hypertension.	Feb 24, 2012 8:59:19 AM
0012	Ngozi Okeke	08034044149	104	105	-1	105.0	104/105	Stage 2 Hypertension.	Feb 24, 2012 8:47:44 AM
0012	Ngozi Okeke	08034044149	107	74	33	85.0	107/74	Desirable or Normal BP.	Feb 24, 2012 8:47:11 AM
0012	Ngozi Okeke	08034044149	107	66	41	80.0	107/66	Desirable or Normal BP.	Feb 24, 2012 9:16:36 AM
0012	Ngozi Okeke	08034044149	110	69	41	83.0	110/69	Desirable or Normal BP.	Feb 24, 2012 9:14:59 AM
0012	Ngozi Okeke	08034044149	111	69	42	83.0	111/69	Desirable or Normal BP.	Feb 24, 2012 9:18:45 AM
0012	Ngozi Okeke	08034044149	113	98	15	103.0	113/98	Stage 1 Hypertension	Feb 24, 2012 9:02:34 AM
0012	Ngozi Okeke	08034044149	116	86	30	96.0	116/86	Prehypertension	Feb 24, 2012 9:19:49 AM

Fig 6: Mobile User log File

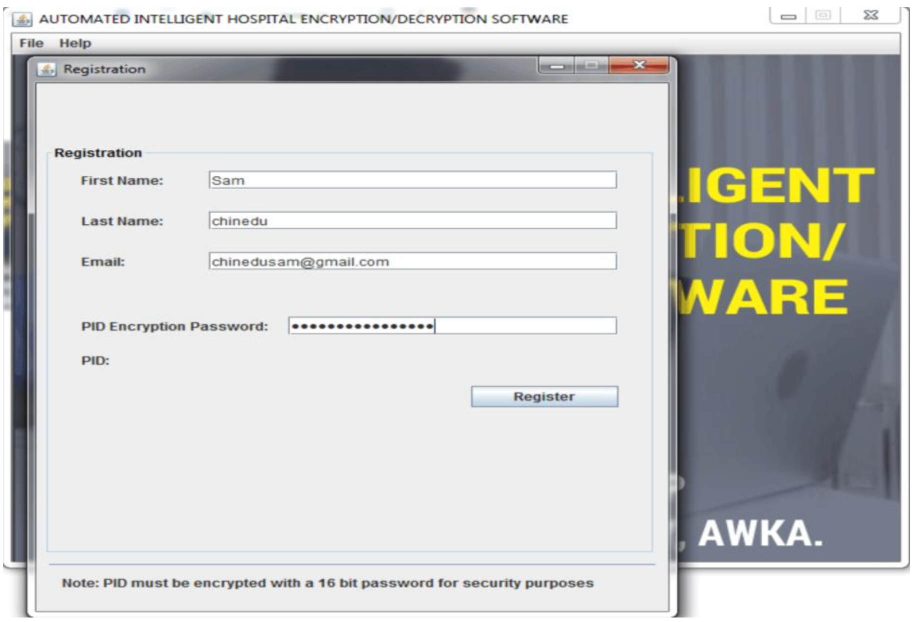


Fig. 7: Patient's Registration

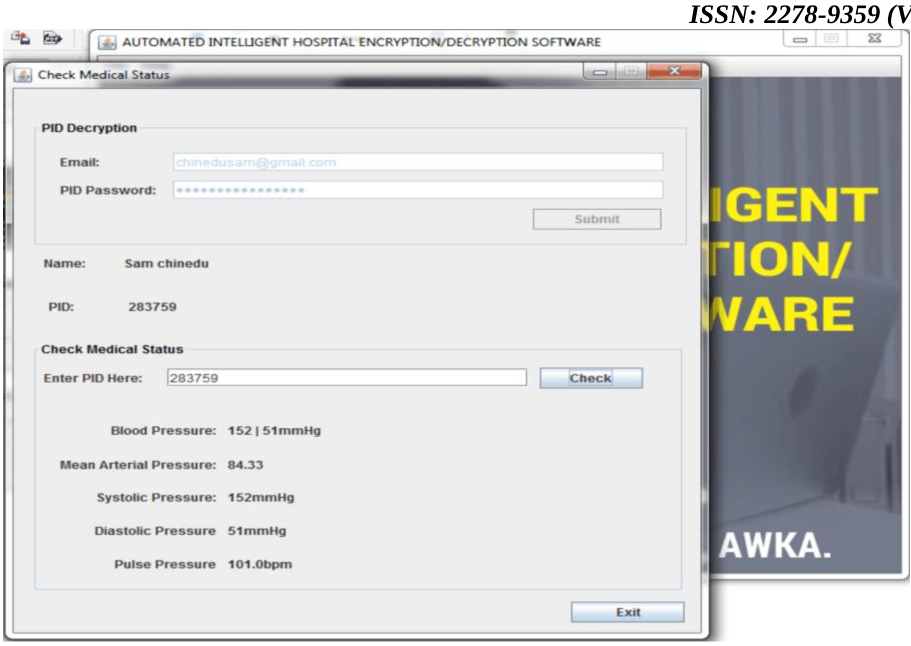


Fig 8: The decryption

V. CONCLUSION

Implementing Internet of things in Remote Patient Medical Monitoring System has been presented. It has been shown that Internet of Things is fully involved in Remote Patient Medical Monitoring System. This is because when patients are remotely monitored, they are embedded with sensors which gather physiological information from the patients and send the results to the server in the hospital where the records are kept and from where the doctor can view each patient's records and proffer solution when the need arises.

In this research work, the patients' medical records were simulated with the IPDA and sent to the server for timely intervention by the doctor. The simulated medical records of the patients were also encrypted to prevent unauthorized access and only decrypted in the server by authorized personnel.

REFERENCES

[1] *An Introduction to the Internet of Things (IoT) (PDF)* Cisco.com. San Francisco, California: Lopez Research. 2013.
[2] *Behind The Numbers: Growth in the Internet of Things*,TheConnectivist 2015.
[3] E. Brown*"Who Needs the Internet of Things?"*. Linux.com 2016.
[4] E. Brown *"21 Open Source Projects for IoT"*. Linux.com 2016.
[5] *Budget 2015: some of the things we've announced*. HM Treasury, 2015.
[6] *Can we expect the Internet of Things in healthcare?*.IoT Agenda, 2016.
[7] Y. Erlich,*"A vision for ubiquitous sequencing"*. Genome Research. 2015 vol. 25 1411–1416. ISSN 1088-9051. PMC 4579324. PMID 26430149. doi:10.1101/gr.191692.115.
[8] M. Ersue, D. Romascanu, J.Schoenwaelder, A. Sehgal "*Management of Networks with Constrained Devices*: Use Cases". IETF Internet Draft 2014.
[9] S. Fickas, G.Kortuem, Z.Segall "Software organization for dynamic and adaptable wearable systems". International Symposium on Wearable Computers 1997: p. 56–63. ISBN 0-8186-8192-6. doi:10.1109/ISWC.1997.629920.
[10] "Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015". Gartner. 10 2015.
[11] M. Hogan. *"The 'The Internet of Things Database' Data Management Requirements"*. ScaleDB. 2014.
[12] *International Telecommunication Union*, Overview of the Internet of things, Recommendation ITU-T Y.2060, 2012
[13] *Internet of Things (IoT)*. gatewaytechnolabs.com.
[14] *Internet of Things Done Wrong Stifles Innovation.*InformationWeek. 2014.
[15] *Internet of Things Global Standards Initiative*. ITU, 2015.
[16] *Internet of Things: Science Fiction or Business Fact? (PDF)*. Harvard Business Review, 2014.
[17] R. Istepanian, S. Hu, N. Philip, A.Sungoor, "The potential of Internet of m-health Things "m-IoT" for non-invasive glucose level sensing". Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). ISBN 978-1-4577-1589-1. doi:10.1109/IEMBS.2011.6091302, 2011.
[18] T. Lindner,"The Supply Chain: Changing at the Speed of Technology". Connected World, 2015.
[19] *Main Report: An In-depth Look at Expert Responses*. Pew Research Center: Internet, Science & Tech. 2014.
[20] F. Mattern, C.Floerkemeiern,"From the Internet of Computers to the Internet of Things" (PDF). Informatik-Spektrum. Vol. **33** (2): p. 107–121, 2010doi:10.1007/s00287-010-0417-7.

[21] F. Mattern, C.Floerkemeier, "From the Internet of Computers to the Internet of Things" (PDF). ETH Zurich. Retrieved 2016.

[22] Molluscan eye, 2015.

[23] *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020*, ABI Research, 2013.

[24] A. Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated". IEEE, 2016.

[25] L. Noto, Guido, I. Walden, "Contracting for the 'Internet of Things': Looking into the Nest". Queen Mary School of Law Legal Studies Research Paper No. 219, 2016. SSRN 2725913 .

[26] J. Pontin ,"ETC: Bill Joy's Six Webs". MIT Technology Review, 2005.

[27] R. Raji, "Smart networks for control". IEEE Spectrum 1994.

[28] A. Reddy,"Reaping the Benefits of the Internet of Things" (PDF). Cognizant 2014.

[29] G. Santucci"The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects" (PDF). European Commission Community Research and Development Information Service 2016.

[30] M. Swan "Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". Sensor and Actuator Networks. Vol. **1** (3), p. 217–253, 2012,doi:10.3390/jsan1030217.

[31] *The Evolution of Internet of Things*, CasaleggioAssociati, 2011.

[32] *The "Only" Coke Machine on the Internet*,Carnegie Mellon University, 2014.

[33] O. Vermesan, P. Friessr,Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems (PDF). Aalborg, Denmark: River Publishers. ISBN 978-87-92982-96-4 2013.

[34] B. Violino"The 'Internet of things' will mean really, really big data". InfoWorld 2014.

[35] M. Weiser "The Computer for the 21st Century" (PDF). Scientific American. Vol. **265** (3), p. 94–104, 1991. Bibcode:1991SciAm.265c..94W. doi:10.1038/scientificamerican0991-94.

[36] I. Wigmore, "Internet of Things (IoT)". TechTarget, 2014.

