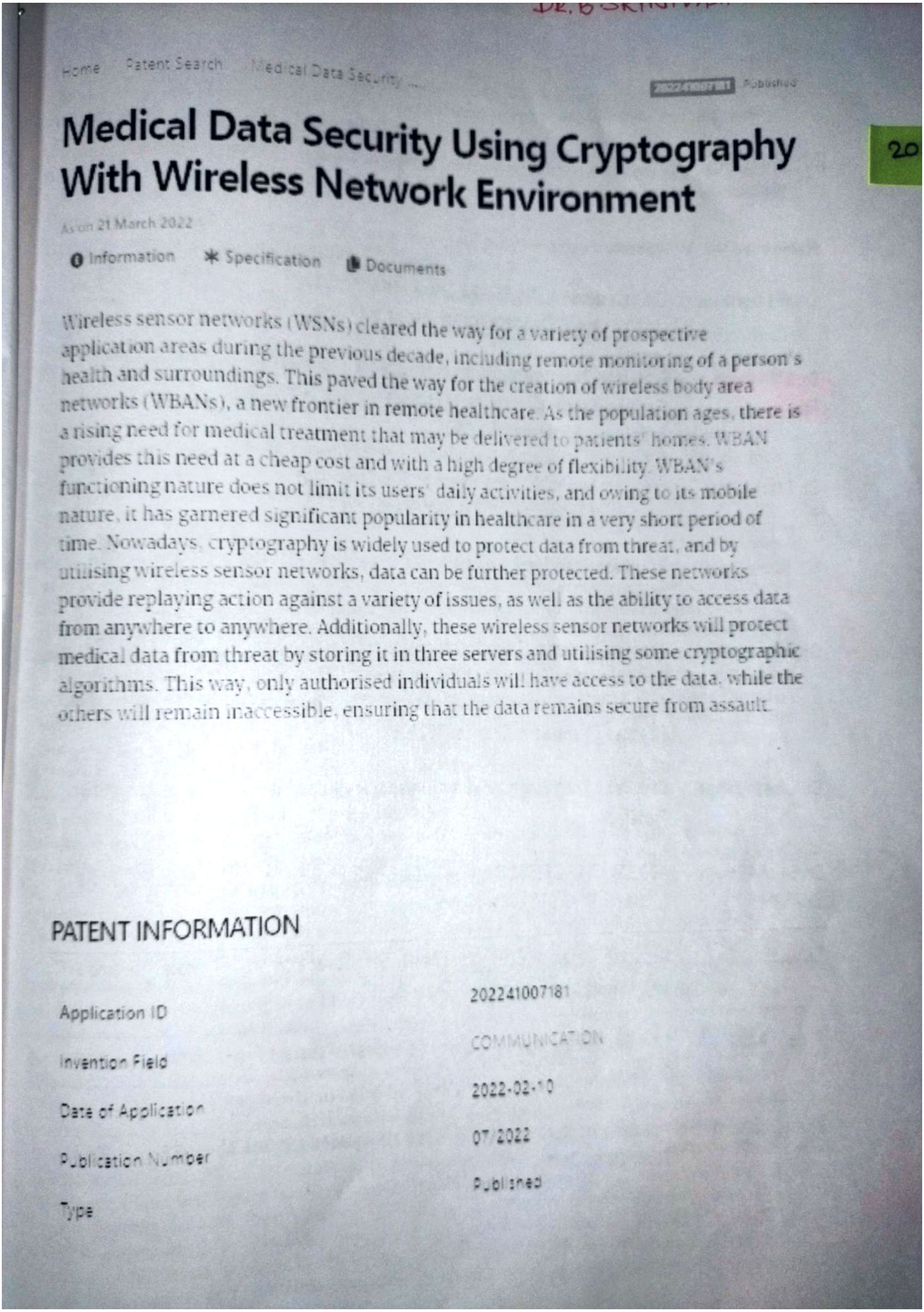
Gokaraju Rangaraju Institute of Engineering and Technology

Department of Computer Science and Engineering

PATENTS

S.No.	Title of the Patent	File Number	Date	Names of the Patenter	Status
2021-22					
1	Medical data security using cryptography with wireless network environment	202241007181	10/02/2022	Dr. B. Srinivasa Rao	2022 Published
2	Machine Learning Model For Predicting Severity Prognosis In Patients Infected With COVID-19	202141032115	13/08/2021	Dr. G. Karuna Dr. Y. Vijayalata Dr G N Beena Bethel Dr Ashlin Deepa R N	2021 Published

DR. B SRINIVA



20

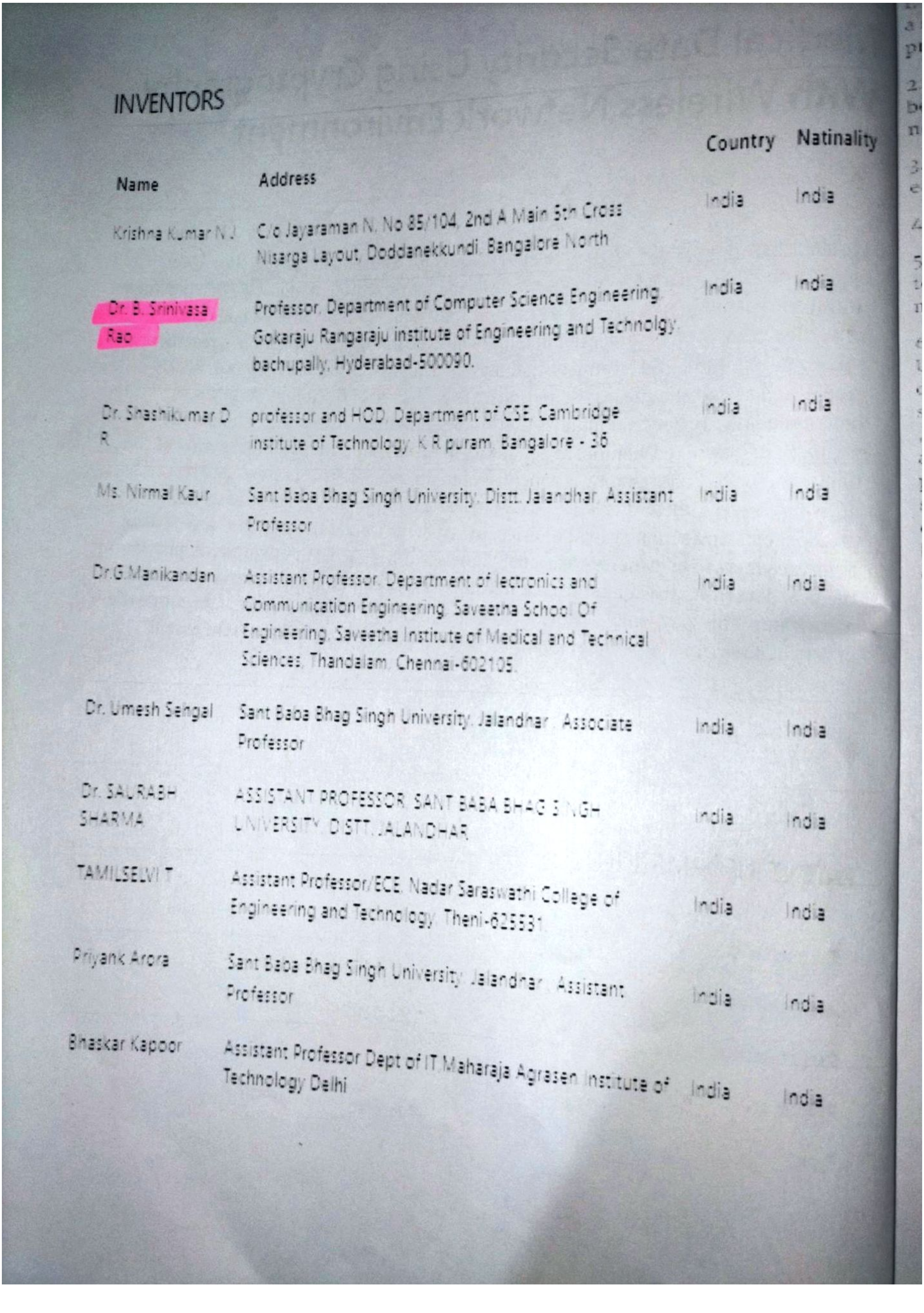
Medical Data Security Using Cryptography With Wireless Network Environment

As on 21 March 2022

Wireless sensor networks (WSNs) cleared the way for a variety of prospective application areas during the previous decade, including remote monitoring of a person's health and surroundings. This paved the way for the creation of wireless body area networks (WBANs), a new frontier in remote healthcare. As the population ages, there is a rising need for medical treatment that may be delivered to patients' homes. WBAN provides this need at a cheap cost and with a high degree of flexibility. WBAN's functioning nature does not limit its users' daily activities, and owing to its mobile nature, it has garnered significant popularity in healthcare in a very short period of time. Nowadays, cryptography is widely used to protect data from threat, and by utilising wireless sensor networks, data can be further protected. These networks provide replaying action against a variety of issues, as well as the ability to access data from anywhere to anywhere. Additionally, these wireless sensor networks will protect medical data from threat by storing it in three servers and utilising some cryptographic algorithms. This way, only authorised individuals will have access to the data, while the others will remain inaccessible, ensuring that the data remains secure from assault.

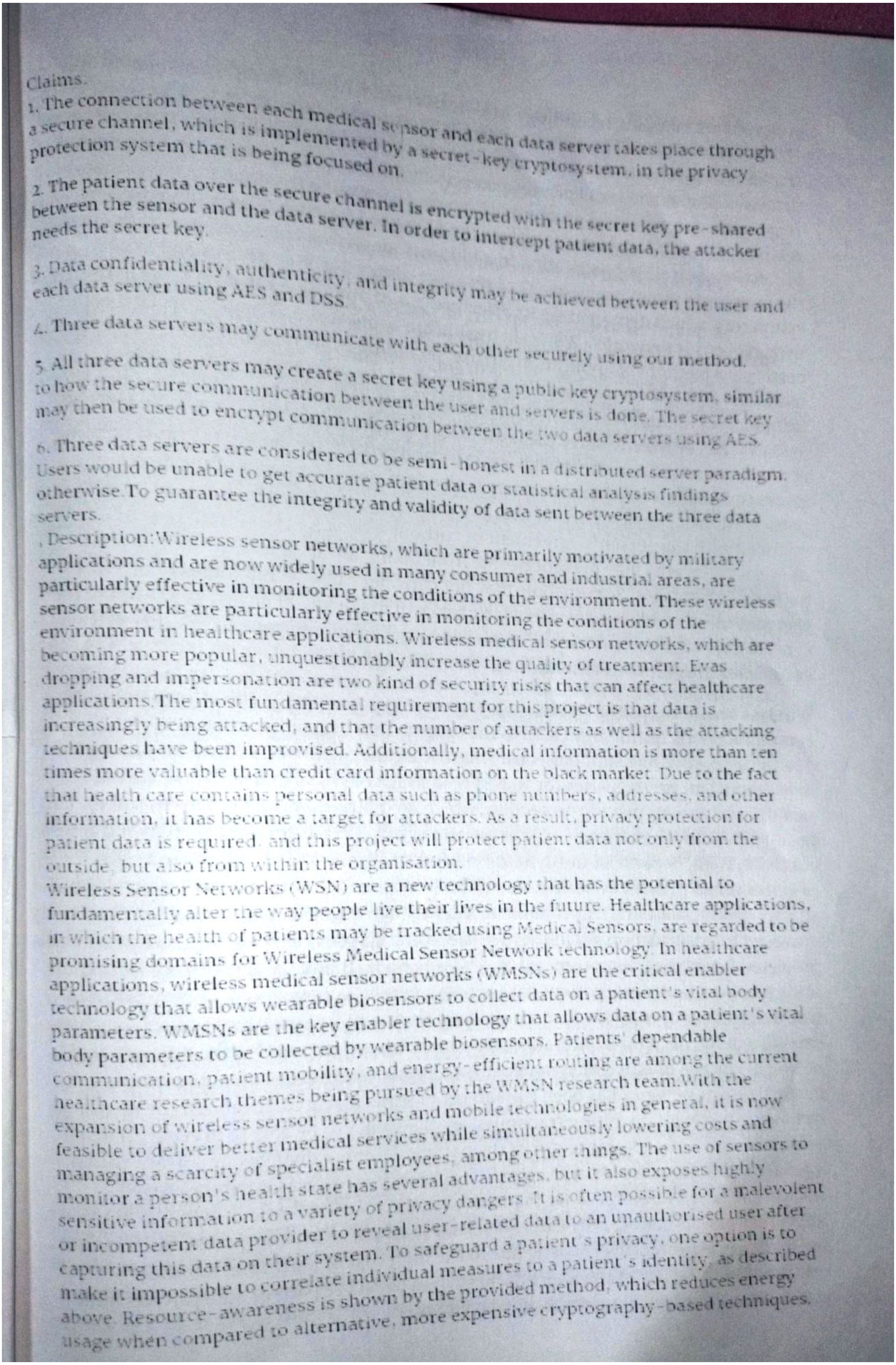
PATENT INFORMATION

Application ID	202241007181
Invention Field	COMMUNICATION
Date of Application	2022-02-10
Publication Number	07/2022
Type	Published



INVENTORS

Name	Address	Country	Natinality
Krishna Kumar N J	C/o Jayaraman N, No 85/104, 2nd A Main 5th Cross Nisarga Layout, Doddanekkundi, Bangalore North	India	India
Dr. B. Srinivasa Rao	Professor, Department of Computer Science Engineering, Gokaraju Rangaraju institute of Engineering and Technolgy, bachupally, Hyderabad-500090.	India	India
Dr. Shashikumar D R	professor and HOD, Department of CSE, Cambridge institute of Technology, K R puram, Bangalore - 36	India	India
Ms. Nirmal Kaur	Sant Baba Bhag Singh University, Distt. Jalandhar, Assistant Professor	India	India
Dr.G.Manikandan	Assistant Professor, Department of lectronics and Communication Engineering, Saveetha School Of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai-602105.	India	India
Dr. Umesh Sehgal	Sant Baba Bhag Singh University, Jalandhar , Associate Professor	India	India
Dr. SAURABH SHARMA	ASSISTANT PROFESSOR, SANT BABA BHAG SINGH UNIVERSITY, DISTT. JALANDHAR	India	India
TAMILSELVI T	Assistant Professor/ECE, Nadar Saraswathi College of Engineering and Technology, Theni-625531.	India	India
Priyank Arora	Sant Baba Bhag Singh University, Jalandhar , Assistant Professor	India	India
Bhaskar Kapoor	Assistant Professor Dept of IT,Maharaja Agrasen Institute of Technology Delhi	India	India



Claims.

1. The connection between each medical sensor and each data server takes place through a secure channel, which is implemented by a secret-key cryptosystem. in the privacy protection system that is being focused on.

2. The patient data over the secure channel is encrypted with the secret key pre-shared between the sensor and the data server. In order to intercept patient data, the attacker needs the secret key.

3. Data confidentiality, authenticity, and integrity may be achieved between the user and each data server using AES and DSS.

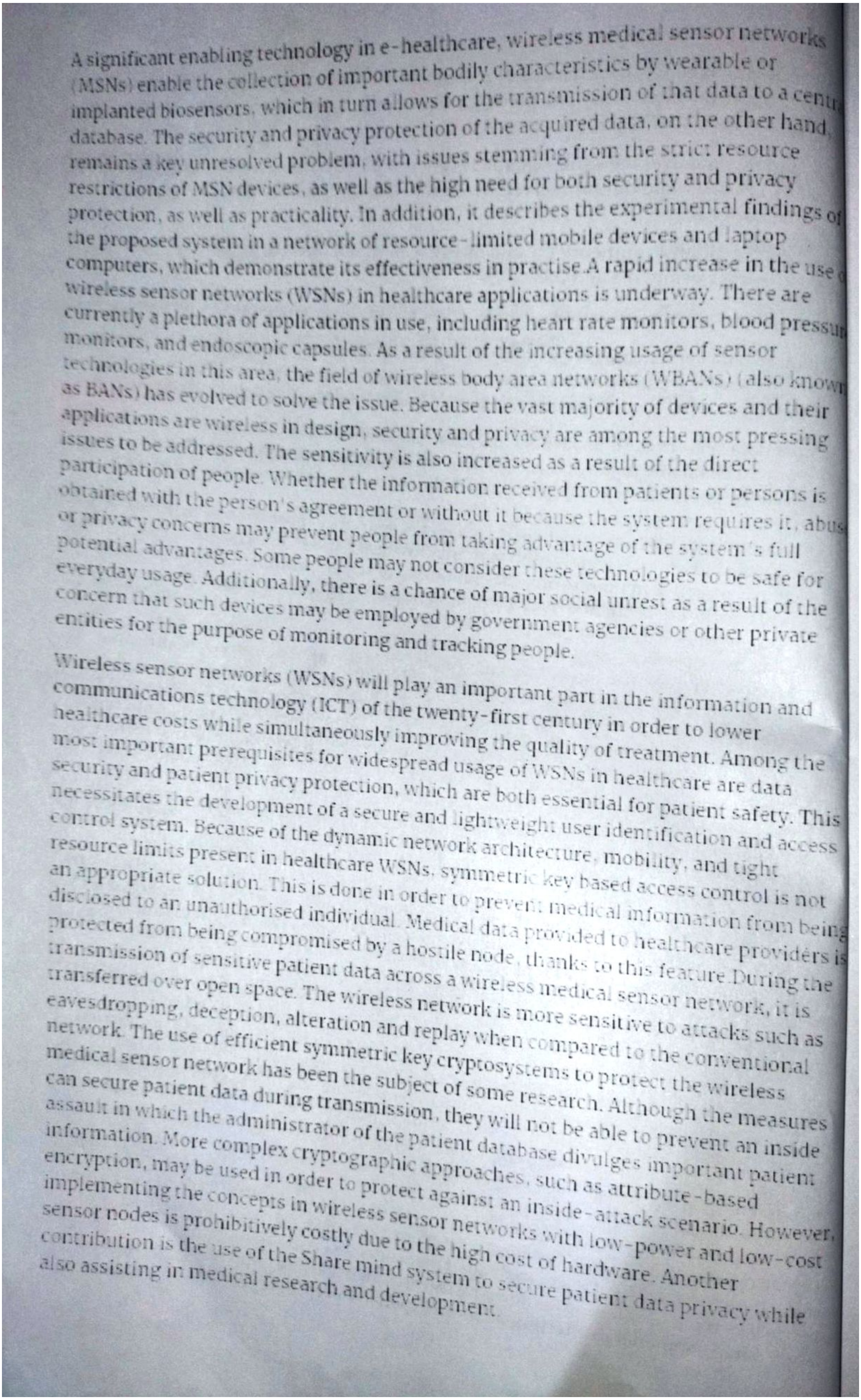
4. Three data servers may communicate with each other securely using our method.

5. All three data servers may create a secret key using a public key cryptosystem, similar to how the secure communication between the user and servers is done. The secret key may then be used to encrypt communication between the two data servers using AES.

6. Three data servers are considered to be semi-honest in a distributed server paradigm. Users would be unable to get accurate patient data or statistical analysis findings otherwise.To guarantee the integrity and validity of data sent between the three data servers.

, Description:Wireless sensor networks, which are primarily motivated by military applications and are now widely used in many consumer and industrial areas, are particularly effective in monitoring the conditions of the environment. These wireless sensor networks are particularly effective in monitoring the conditions of the environment in healthcare applications. Wireless medical sensor networks, which are becoming more popular, unquestionably increase the quality of treatment. Evas dropping and impersonation are two kind of security risks that can affect healthcare applications.The most fundamental requirement for this project is that data is increasingly being attacked, and that the number of attackers as well as the attacking techniques have been improvised. Additionally, medical information is more than ten times more valuable than credit card information on the black market. Due to the fact that health care contains personal data such as phone numbers, addresses, and other information, it has become a target for attackers. As a result, privacy protection for patient data is required. and this project will protect patient data not only from the outside, but also from within the organisation.

Wireless Sensor Networks (WSN) are a new technology that has the potential to fundamentally alter the way people live their lives in the future. Healthcare applications, in which the health of patients may be tracked using Medical Sensors, are regarded to be promising domains for Wireless Medical Sensor Network technology. In healthcare applications, wireless medical sensor networks (WMSNs) are the critical enabler technology that allows wearable biosensors to collect data on a patient's vital body parameters. WMSNs are the key enabler technology that allows data on a patient's vital body parameters to be collected by wearable biosensors. Patients' dependable communication, patient mobility, and energy-efficient routing are among the current healthcare research themes being pursued by the WMSN research team.With the expansion of wireless sensor networks and mobile technologies in general, it is now feasible to deliver better medical services while simultaneously lowering costs and managing a scarcity of specialist employees, among other things. The use of sensors to monitor a person's health state has several advantages, but it also exposes highly sensitive information to a variety of privacy dangers. It is often possible for a malevolent or incompetent data provider to reveal user-related data to an unauthorised user after capturing this data on their system. To safeguard a patient's privacy, one option is to make it impossible to correlate individual measures to a patient's identity, as described above. Resource-awareness is shown by the provided method, which reduces energy usage when compared to alternative, more expensive cryptography-based techniques.



A significant enabling technology in e-healthcare, wireless medical sensor networks (MSNs) enable the collection of important bodily characteristics by wearable or implanted biosensors, which in turn allows for the transmission of that data to a centr database. The security and privacy protection of the acquired data, on the other hand, remains a key unresolved problem, with issues stemming from the strict resource restrictions of MSN devices, as well as the high need for both security and privacy protection, as well as practicality. In addition, it describes the experimental findings of the proposed system in a network of resource-limited mobile devices and laptop computers, which demonstrate its effectiveness in practise.A rapid increase in the use o wireless sensor networks (WSNs) in healthcare applications is underway. There are currently a plethora of applications in use, including heart rate monitors, blood pressur monitors, and endoscopic capsules. As a result of the increasing usage of sensor technologies in this area, the field of wireless body area networks (WBANs) (also known as BANs) has evolved to solve the issue. Because the vast majority of devices and their applications are wireless in design, security and privacy are among the most pressing issues to be addressed. The sensitivity is also increased as a result of the direct participation of people. Whether the information received from patients or persons is obtained with the person's agreement or without it because the system requires it, abus or privacy concerns may prevent people from taking advantage of the system's full potential advantages. Some people may not consider these technologies to be safe for everyday usage. Additionally, there is a chance of major social unrest as a result of the concern that such devices may be employed by government agencies or other private entities for the purpose of monitoring and tracking people.

Wireless sensor networks (WSNs) will play an important part in the information and communications technology (ICT) of the twenty-first century in order to lower healthcare costs while simultaneously improving the quality of treatment. Among the most important prerequisites for widespread usage of WSNs in healthcare are data security and patient privacy protection, which are both essential for patient safety. This necessitates the development of a secure and lightweight user identification and access control system. Because of the dynamic network architecture, mobility, and tight resource limits present in healthcare WSNs, symmetric key based access control is not an appropriate solution. This is done in order to prevent medical information from being disclosed to an unauthorised individual. Medical data provided to healthcare providers is protected from being compromised by a hostile node, thanks to this feature.During the transmission of sensitive patient data across a wireless medical sensor network, it is transferred over open space. The wireless network is more sensitive to attacks such as eavesdropping, deception, alteration and replay when compared to the conventional network. The use of efficient symmetric key cryptosystems to protect the wireless medical sensor network has been the subject of some research. Although the measures can secure patient data during transmission, they will not be able to prevent an inside assault in which the administrator of the patient database divulges important patient information. More complex cryptographic approaches, such as attribute-based encryption, may be used in order to protect against an inside-attack scenario. However, implementing the concepts in wireless sensor networks with low-power and low-cost sensor nodes is prohibitively costly due to the high cost of hardware. Another contribution is the use of the Share mind system to secure patient data privacy while also assisting in medical research and development.

This includes the establishment of a doctor node and connecting it to the sensor and server nodes, as well as uploading files and dividing and encrypting them, and then having the doctor node decrypt and download them. Examples of these screens may be seen from Fig.3 to Fig.9.In privacy protection system focused in. the communication between each medical sensor and each data server is through a secure channel, which is implemented by a secret-key cryptosystem. The patient data over the secure channel is encrypted with the secret key pre-shared between the sensor and the data server. Without the secret key, the attacker cannot eaves- drop the patient data. To protect uploaded data against inside attacks, servers can encrypt once. Here servers apply Elgamal encryption using Elgamal Public Key. So these uploaded sensed data have more security against inside attacks. The doctor wants to access these uploaded sensed data. So he downloads all sensed data from all 3 servers.First he decrypts the sensed data based on Elgamal decryption using Elgamal Private Key After Elgamal Decryption, doctor decrypts the sensed data based on Paillier Decryption using

Paillier Private Key.Finally he gets the original sensed data. By AES and DSS, this can achieve data confidentiality, authenticity and integrity between the user and each data server. In our solution, the communications among three data servers can be also through secure channels. Like the secure communication between the user and the data servers, any two of the three data servers can establish a secret key with a public key cryptosystem. Then the communication between the two data servers can be encrypted with AES based on the secret key.In distributed server model, the three data servers are assumed to be semi-honest. Otherwise, the user can never obtain correct patient data and statistical analysis results. To ensure data authenticity and integrity in the communications among the three data servers.

Conclusion:

In this investigation is done to security and privacy issues in the medical sensor data collection, storage and queries and presented a complete solution for privacy preserving medical sensor network. To secure the communication between medical sensors and data servers, use of the lightweight encryption scheme and MAC generation scheme based on SHA-3 proposed. To keep the privacy of the patient data, a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the patient data can be preserved. For the legitimate user (e.g., physician) to access the patient data, an access control protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. For the legitimate user (e.g., medical researcher) to perform statistical analysis on the patient data, proposed some new protocols for average, correlation, variance and regression analysis, where the three data servers cooperate to process the patient data without disclosing the patient privacy and then provide the user with the statistical analysis results. Security and privacy analysis has shown that our protocols are secure against both outside and inside attacks as long as one data server is not compromised. Performance analysis has shown that our protocols are practical as well. Unlike, our solution can preserve the patient data privacy as long as one of three data server is not compromised.

There are three data servers in this model's architecture. In Fig. 1, they are shown. This is the beginning of the deployment process for each medical sensor and the servers that store the data collected from them. Three secret keys are pre-deployed and pre-shared with three data servers for each medical sensor. Using a secret key, sensors communicate with a single data server through an encrypted channel. Wireless medical sensor networks are made possible by the distributed server concept. In addition to sensors and servers, there is a "doctor" node. A patient wears a sensor node that transmits physiological data to three servers. In this case, the doctor may view the data on the server.

Doctors are initially connected to sensor nodes and servers in a distributed server topology. Dr. Paillier and Dr. Elgamal produce the Paillier and Elgamal Public and Private Keys during the connection period. Paillier and Elgamal public keys should be sent to servers and nodes, respectively, for Paillier Encryption. Sensor nodes collect information about the body's health.Split the data into three separate chunks for each server.These blocks are then encrypted using Paillier's Public Key. These encrypted chunks are then sent to three different servers.Servers may encrypt submitted data just once in order to protect it against assaults from the inside. Elgamal Public Key is used to encrypt data on these servers. As a result, the uploaded sensed data are more resistant to assaults from the inside.In this module, the doctor wishes to view the detected data that has been submitted. Consequently, all three servers' detected information is downloaded. To begin, he uses Elgamal decryption and the Elgamal Private Key to decode the detected data. After Elgamal Decryption, the doctor uses Paillier Decryption and the Paillier Private Key to decode the detected data. Finally, he receives the original data. Dr. Taher El Gamal's public-key cryptography system, El Gamal, is the primary cryptography technology we'll be relying on for this project. Elgamal This implies that El Gamal relies on the one-way function, which separates encryption and decryption. Two modular exponentiations are required for the encryption procedure (extra time).A secret-key cryptosystem provides a secure connection between each medical sensor and each data server. Using a secret key pre-shared between the sensor and the data server, the patient data is sent through the secure channel. The attacker can't listen in on patient data unless they have the secret key.

1. Data Collection Protocol

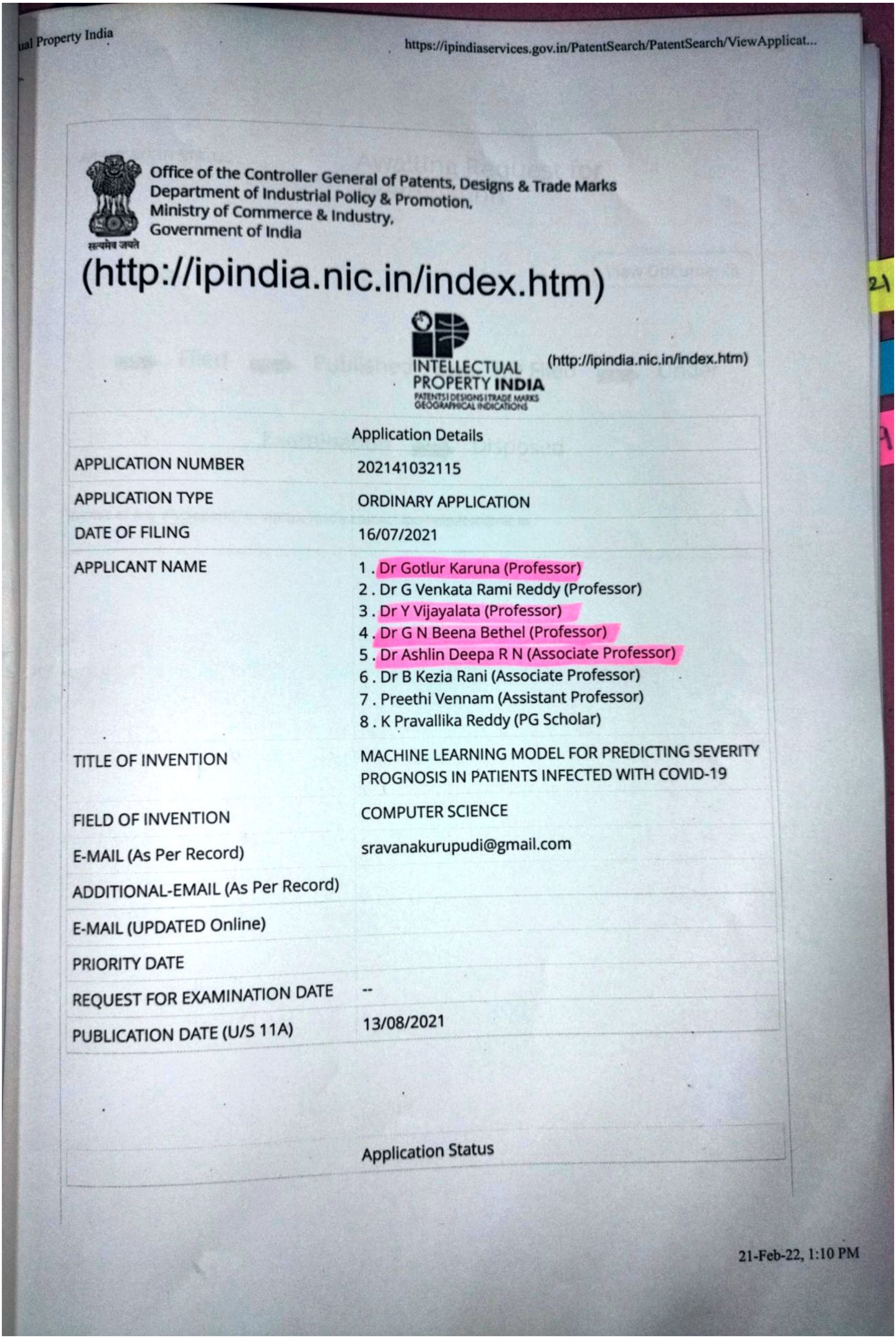
Each medical sensor and each data server must go through an initial deployment process. Three secret keys are pre-deployed and pre-shared with three data servers for each medical sensor. Using a secret key, sensors communicate with a single data server through an encrypted channel. Pre-deployed in each sensor is a secret key that can create random numbers. Consider the fact that various medical sensors have unique secret codes.

2. Access control protocol

Furthermore, it is supposing that the user has set up three channels, each with an own set of data servers. When requesting patient data, the user must utilise one of three secure channels to submit a request to each of the three data servers, each of which requires the user to transmit a signature on the query and a digital certificate.

3. Statistical Analysis Protocols

Patients' personal information is safeguarded not only through access control but also through privacy-preserving statistical analysis of patient data for medical research, in which three data servers work together to assist the medical researcher in analysing the patient data without disclosing the patient's identity.



ual Property India

https://ipindiaservices.gov.in/PatentSearch/PatentSearch/ViewApplicat...

Office of the Controller General of Patents, Designs & Trade Marks
Department of Industrial Policy & Promotion,
Ministry of Commerce & Industry,
Government of India

(http://ipindia.nic.in/index.htm)

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

(http://ipindia.nic.in/index.htm)

21

Application Details	
APPLICATION NUMBER	202141032115
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	16/07/2021
APPLICANT NAME	1 . Dr Gotlur Karuna (Professor) 2 . Dr G Venkata Rami Reddy (Professor) 3 . Dr Y Vijayalata (Professor) 4 . Dr G N Beena Bethel (Professor) 5 . Dr Ashlin Deepa R N (Associate Professor) 6 . Dr B Kezia Rani (Associate Professor) 7 . Preethi Vennam (Assistant Professor) 8 . K Pravallika Reddy (PG Scholar)
TITLE OF INVENTION	MACHINE LEARNING MODEL FOR PREDICTING SEVERITY PROGNOSIS IN PATIENTS INFECTED WITH COVID-19
FIELD OF INVENTION	COMPUTER SCIENCE
E-MAIL (As Per Record)	sravanakurupudi@gmail.com
ADDITIONAL-EMAIL (As Per Record)	
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	--
PUBLICATION DATE (U/S 11A)	13/08/2021

Application Status

21-Feb-22, 1:10 PM