iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Secure Patient State Supervisor in Medical Sensor Networks

Sagar D C[1]
[1]Department of Information Science and Engineering S J B Institute of Technology, Bengaluru, Karnataka, India

Abstract - Wireless sensor networks have been evolved to support patients in health care domain. Data of the patients can be collected by the implantable or wearable sensor devices. Collected data will be transmitted to doctor's present in remote place. The major issue in transmission is the security and privacy protection of the collected data because of the resource constraints in the medical sensor network devices. There is a high demand for both security and privacy in practicality. Hence, in this paper we proposed a secure agent based approach for providing the security and privacy over data transmission. We analyze the proposed approach for data authenticity and attacks, it is efficient and feasible
Keywords: wireless sensor networks, body sensors, data transmission, security, authenticity

I. INTRODUCTION

Wireless medical sensor networks have emerged as a promising technique which will revolutionize the way of seeking healthcare at home, hospital, or large medical facilities. Instead of being measured face-to-face, with MSNs, patient's health related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, insurance companies, and patients. Through this way, healthcare processes, such as clinical diagnosis and emergency medical response, will be facilitated and expedited, thereby greatly increasing the efficiency of healthcare.

Sensor networks have the potential to greatly impact many aspects of medical care. By outfitting patients with wireless, wearable vital sign sensors, collecting detailed real-time data on physiological status can be greatly simplified. However, there is a significant gap between existing sensor network systems and the needs of medical care. In particular, medical sensor networks must support multicast routing topologies, node mobility, a wide range of data rates and high degrees of reliability, and security.

The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at proximity of the user. The implantable medical devices are those that are inserted inside human body. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body- area networks can collect information about an individual's health, fitness, and energy expenditure.

A. Wearable Biosensors

Wearable biosensor systems for health monitoring are an emerging trend and are expected to enable proactive personal health management and better treatment of various medical conditions. These systems, comprising various types of small physiological sensors, transmission modules and processing capabilities, promise to change the future of health care, by providing low-cost wearable unobtrusive solutions for continuous all-day and any-place health, mental and activity status monitoring.

B. Implantable sensors

Implantable sensor systems offer great potential for enhanced medical care and improved quality of life, consequently leading to vast investment in this exciting field. Implantable sensor systems for medical applications provides a wide-ranging overview of the core technologies, key challenges and main issues related to the development and use of these devices in a diverse range of medical applications. Implantable systems need to be small, lightweight, and sealed from the harsh environment of the human body. These systems should also consume very little power to allow for long-term operation, and they need to provide for data transmission to and from the implanted device.

This paper is framed as follows: Section II discusses about related work. In section III, proposed scheme is represented and

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

discussed in detail. In section IV, gives the implementation details and snapshots obtained in this work. Conclusion is presented in section V.

II. RELATED WORK

In late years, imaginative wellbeing focused systems administration and remote correspondence advancements have been produced, which turned into a characteristic piece of numerous current restorative gadgets. The implantable therapeutic gadgets (IMDs) [3], including pacemakers, heart defibrillators, insulin pumps, neurostimulators, and so on., use their remote radios to convey opportune patient data, driving to a superior social insurance checking framework. Current advances make it conceivable to send battery-fueled scaled down IMDs on, in, or around the human body for long haul social insurance checking [4]. IMDs report their information to an information sink by remote correspondence channels. The information sink can be an IMD intended to store information or, then again, a cell phone, which can speak with a remote medicinal services office through cell systems or the Web. Every one of those IMDs, which will later be basically alluded as sensors, and the information sink together comprise a little scale remote sensor organize, called a Wireless Body Area Network (WBAN). WBAN as a key empowering procedure for E-social insurance frameworks makes constant wellbeing related data available to therapeutic pros, who are then empowered to cast suitable and opportune restorative treatment to the patients. The taking off national wellbeing consumptions and raising age-related incapacities are moving the accentuation from the healing center to the home [5], which makes WBANs a flawless contender for empowering in-home observing and conclusion, particularly for individuals having endless ailments. Not at all like customary sensor arranges, a WBAN manages more delicate and vital patient data that has critical security, protection, and wellbeing concerns, which may forestall the wide selection of this innovation [6].

Be that as it may, there are difficulties all over the place: Data ought to be transmitted in a protected channel, and we know the difficulties in securing remote correspondence channels. Hub confirmation is the most key venture towards a BAN's underlying trust foundation, key era, what's more, consequent secure interchanges. There exist consider that empowers installed sensors to set up a session key with each other by use physiological flags, for example, Electrocardiograph (ECG) [7], [8], [9], [10], [11], [12], [13], [14], [15]. Additionally, we can pre-disperse keys or privileged insights in sensors if fundamental. From the point of view of cryptography, the high calculation cost of awry cryptography leaves symmetric encryption as the main reasonable choice. Be that as it may, the key-dispersion in symmetric encryption is testing. What's more, symmetric encryption is not a decent decision for broadcasting a message since it includes some trying issues, for example, key-administration and get to control. At the same time, because of the restriction of memory space in sensors, an information sink, which has impressively bigger memory and calculation power, is utilized to store information. To guarantee the security of the information, we need certain level of insurance to the information sink. Notwithstanding, a cell phone like gadget filling in as the information sink can be physically lost or stolen, and an assailant can read the information once he catches the gadget. Besides, late research uncovered that cell phones experience the ill effects of serious security worries since numerous applications regularly go too far and read delicate information at their through and through freedom.

III. PROPOSED WORK

In this section, we proposed a secure patient data transmission scheme. Fig. 1 shows the proposed medical sensor network architecure. This scheme consists of following steps:

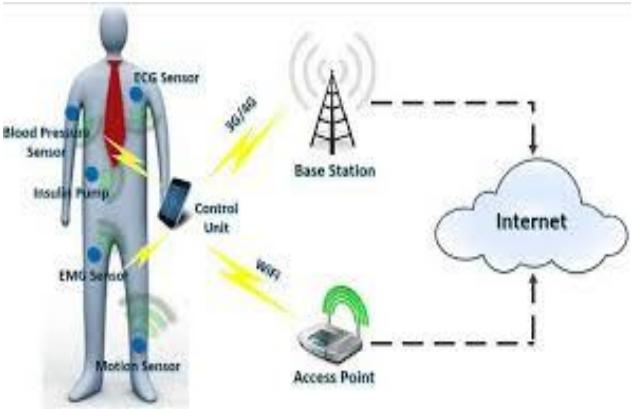


Fig. 1: proposed medical sensor network architecure

A. Step 1: System Initialization

1) In the first step randomly select two large safe prime numbers p and q then compute the public modulus n which is a product of two prime's p and q.

2) In the second step choose a pair of integers e and d which satisfying the properties i.e. product of e and d modulus Euler's totient function strictly equal to one. Euler's totient function is (p-1)(q-1).

3) Here public key is the combination of public modulus n and e, the private key is d value.

4) For every Patient Area Network the secret key is set which is calculated using public one way hash function h() such as SHA-1.

B. *Step 2: Patient Registration and proxy key generation*

1) The user who wants to access the patient health information in the medical server should register their details.

2) After registration, the unique proxy key is generated for the user by the medical server.

3) The proxy key named v which is calculated using warrant, public modulus n and integer d.

4) At last the proxy key is verified using the product of v to the power e and warrant modulo n which is strictly equal to 1. Finally, the proxy key returns to the user

C. Step3: Transmission of Patient Health Information to Network Server

1) The patient health information like body temperature, blood pressure, blood glucose level, heart beat rate is collected by sensors.

2) Due to low power, each time the sensor nodes transmits the patient health data to the network server.

3) When the medical data sent from sensor to controller the unique hash key is generated with the patient health information.

4) The hash key is generated using SHA-1 public one way hash function.

5) For every transmission, the hash key gets updated.

6) When the medical server receives the patient health data, it stores the patient medical data with the original hash key.

D. Step4: Controller Authentication

1) In this module, during every transmission of patient health information from biosensors security techniques are provided.

2) When data transfer from biosensor it reaches the controller.

3) It requests the controller to send the data to the medical server.

4) If the controller accepts the request then the data sent to the medical server.

5) The same process is repeated when the user want to access the data in the medical server.

E. Step5: Retrieval of Patient Health Information from Network Server

The user retrieves the medical data of the patient from the medical server.

1) During registration, the user received the proxy key from the medical server. Using the proxy key he/she can able to login into the system.

2) The user is authenticated u

3) Comparison takes place between the proxy key which is stored in the network server during registration and current proxy key. If it equals the required Patient medical data is displayed by the network server.

IV. IMPLEMENTATION

The implementation of the proposed scheme is made using java language. We have used netbeans IDE for graphical user interface and building the logic. To process the data, we have installed MySQL. First, we collected various patients' data such as patient blood pressure, sugar, heart rate and so on. In order to test, application is deployed in servers and fed data for validation. Necessary security check has been made for verification. Fig. 2 shows the screen shot of the system initialization component. Fig.

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

3 shows the patient health information viewed by the authorized doctor. Fig. 4 shows the patient health parameter

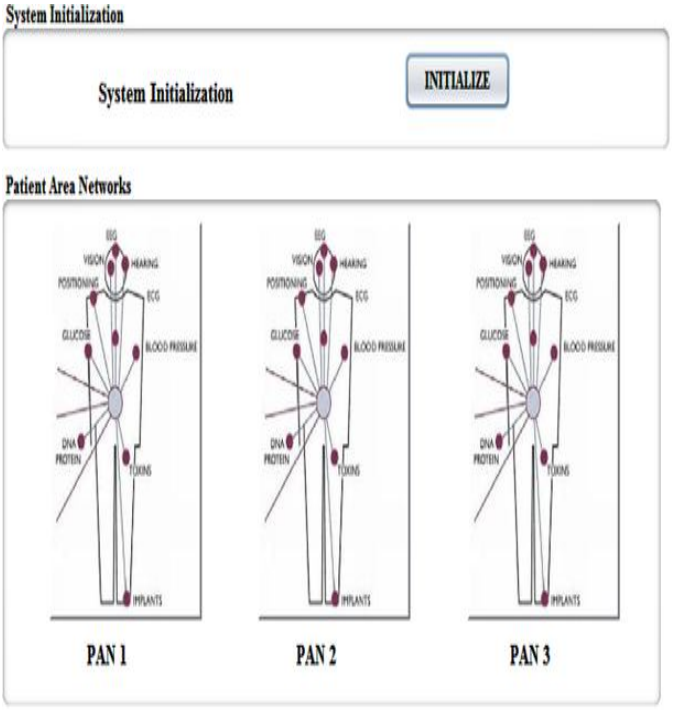
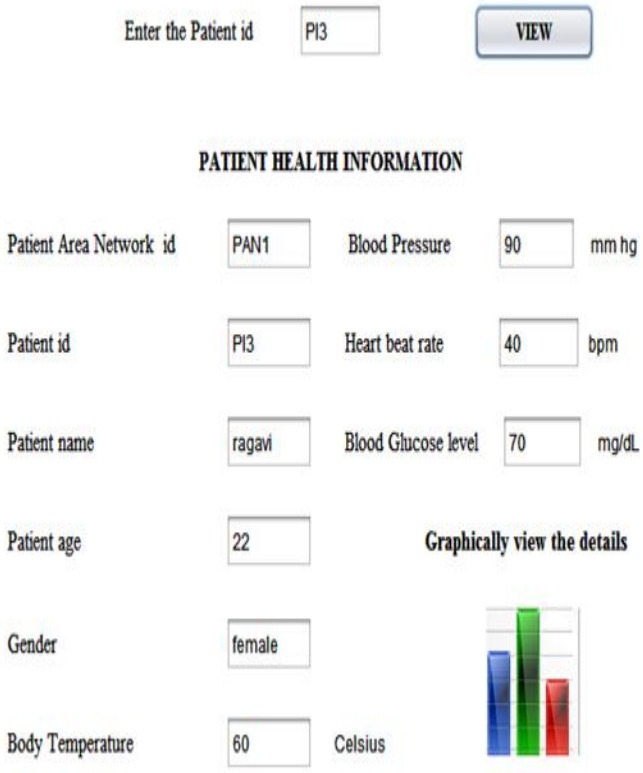


Fig. 2: Screen shot of the system initialization



Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig. 3 Screen shot of the patient health information viewed by the authorized doctor.

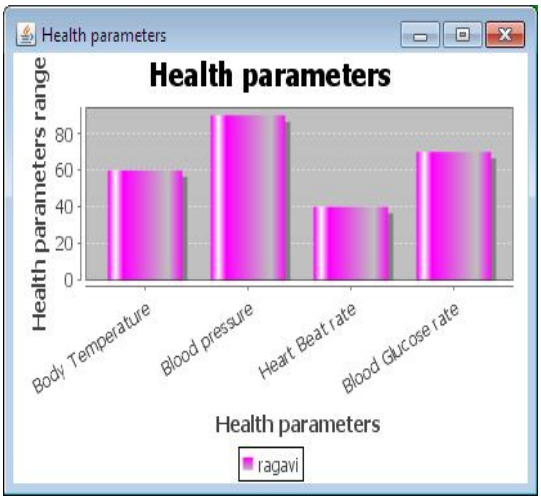


Fig. 4 Graph representation of the patient health parameter

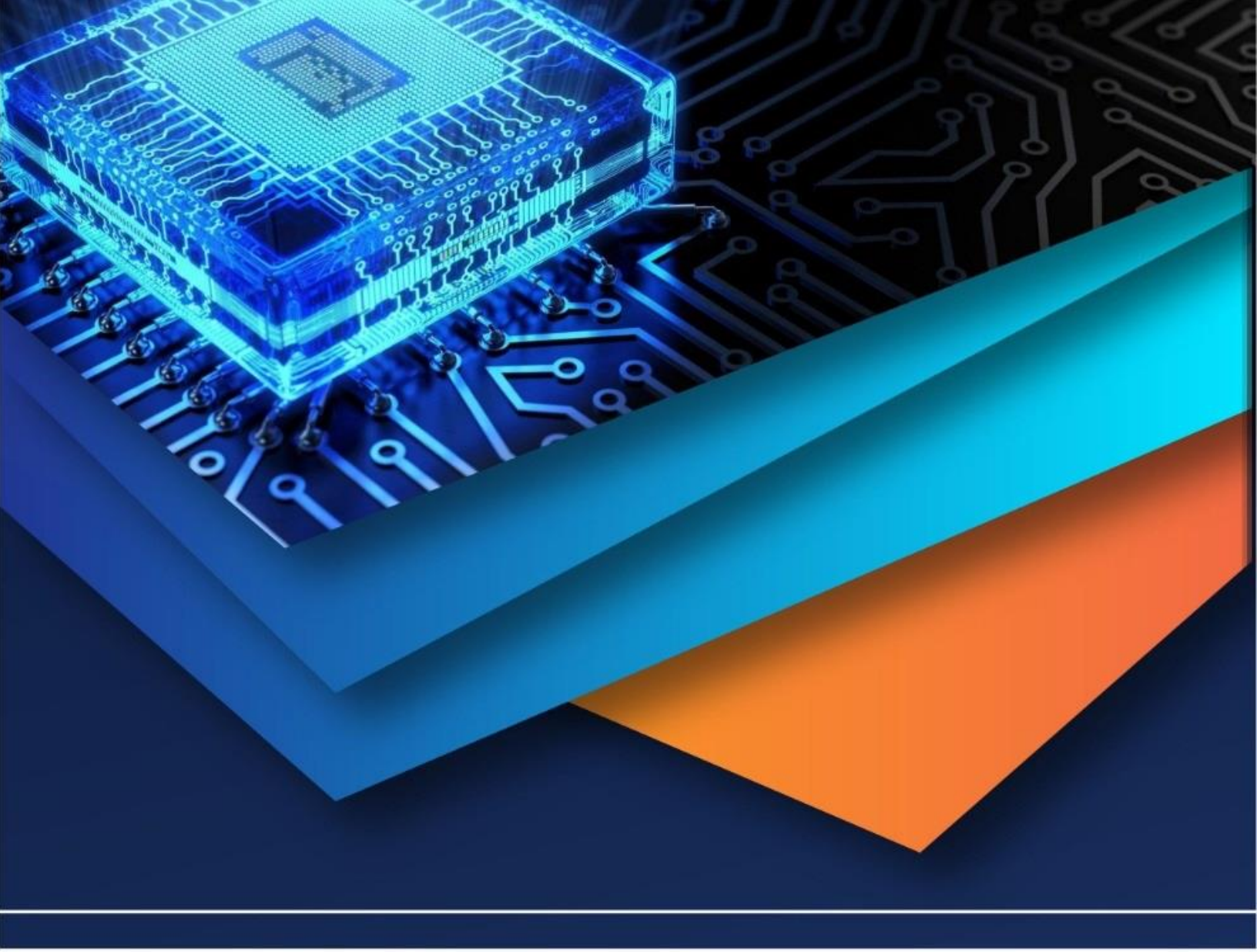
V. CONCLUSION

In the proposed system, we used a hash-chain based key mechanism. Because of this security technique the data transmission from sensor to medical server done in a secure manner. The adversary not able to collect any patient health data or inject any polluted data into the sensor during transmission. In each and every transmission the hash key gets updated. The original key is known only to sender and receiver. The other security technique we used here is proxy protected signature technique. In this technique, the user who wants to access the patient's medical data must contain a valid proxy key. The proxy key is generated during registration itself. Using that proxy key, he/she can able to enter into the system. Because of this security technique other than the users who are valid are not able to view the patient's medical data. The two security techniques such as hash-chain based key mechanism and proxy key signature technique achieves the goal

REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
[2] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.
[3] D. Panescu, "Emerging technologies [wireless communication systems for implantable medical devices]," Engineering in Medicine and Biology Magazine, IEEE, vol. 27, no. 2, pp. 96–101, 2008
[4] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in INFOCOM. IEEE, 2012, pp. 388–396
[5] S. Ali, V. Sivaraman, and D. Ostry, "Zero reconciliation secret key generation for body-worn health monitoring devices," in ACM Wisec. ACM, 2012, pp. 39–50.
[6] L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: body area network authentication exploiting channel characteristics," in ACM Wisec. ACM, 2012, pp. 27–38.
[7] C. Poon, Y. Zhang, and S. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Communications Magazine, vol. 44, no. 4, pp. 73–81, 2006.
[8] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," IEEE Transactions on Information Technology in Biomedicine, vol. 14, no. 1, pp. 60–68, 2010.
[9] "EKG-based key agreement in body sensor networks," in INFOCOM Workshops 2008. IEEE, 2008, pp. 1–6.
[10] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in Parallel Processing Workshops, 2003 International Conference on, 2003, pp. 432–439.
[11] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Plethysmogrambased secure inter-sensor communication in body area networks," in Military Communications Conferenc, 2008, pp. 1–7
[12] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in INFOCOM, 2013.
[13] J. Zhou, Z. Cao, and X. Dong, "Bdk: secure and efficient biometric based deterministic key agreement in wireless body area networks," in Proceedings of the 8th International Conference on Body Area Networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013, pp. 488–494.
[14] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data

scrambling," EURASIP Journal on Advances in Signal Processing, vol. 2008, p. 109, 2008.
[15] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: A fuzzy attribute-based signcryption scheme," to appear in IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Emerging Technologies in Communications, 2012
[16] L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: body area network authentication exploiting channel characteristics," in ACM Wisec. ACM, 2012, pp.27-38.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY