iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 9 **Issue:** XII **Month of publication:** December 2021

**DOI:** https://doi.org/10.22214/ijraset.2021.39336

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 9 Issue XII Dec 2021- Available at www.ijraset.com*

# Differential Privacy Preserving in Big data Analytics for Body Area Networks

Adam Gowri Shankar[1], Dr. V. Janardhan Babu[2]
[1]*Research scholar, Department of CSE, Sri Venkatesa Perumal College Of Engineering & Technology (Autonomous) RVS Nagar, KN Road, Puttur, Chittoor (Dist.) – 517 583*
[2]*Professor, Department of CSE, Sri Venkatesa Perumal College Of Engineering & Technology (Autonomous) RVS Nagar, KN Road, Puttur, Chittoor (Dist.) – 517 583*

***Abstract: Body Area Networks (BANs), collects enormous data by wearable sensors which contain sensitive information such as physical condition, location information, and so on, which needs protection. Preservation of privacy in big data has emerged as an absolute prerequisite for exchanging private data in terms of data analysis, validation, and publishing. Previous methods and traditional methods like k-anonymity and other anonymization techniques have overlooked privacy protection issues resulting to privacy infringement. In this work, a differential privacy protection scheme for 'big data in body area network' is developed. Compared with previous methods, the proposed privacy protection scheme is best in terms of availability and reliability. Exploratory results demonstrate that, even when the attacker has full background knowledge, the proposed scheme can still provide enough interference to big sensitive data so as to preserve the privacy.***
***Keywords: BAN's, Privacy, Differential Privacy, Noisy response***

## I. INTRODUCTION

Body area networks (BAN) is also called as Body Sensor Networks (BSN) is becoming more and more important for the whole society nowadays. Modern healthcare related technologies and many other fields' key technologies depend on it. BAN has numerous applications. One of them, medical monitoring applications have the particular hardware and network requirements to ensure their functions and to solve encountered problems. Sensor, battery, and processor +have developed BAN. The security of BAN is another extremely critical issue.

Body Area Networks (BAN) Technology has numerous applications. The main applications are utilized in the medical domain but this technology will not be restricted only to the medical applications, non-medical applications are also predicted. Applications can be composed into three classes:

### *A. Healthcare Sensor Networks Applications*

BAN's have been widely used in the medical healthcare field. It makes physiological monitoring of patient much simpler, less expensive and less authoritative for the patients.

1) *Entertainment:* Multimedia and gaming applications, video streaming, data file transfer, sports, 3D video is one of the possible.
2) *Assistance to People with Disabilities:* The BAN can likewise help the general population with handicaps, for example, muscle pressure screen, dazzle, speech disability, and artificial hands.

### *B. The Composition of body area Sensors*

A body area sensor is formed by:

1) *Sensor/Actor:* It is utilized to measure the vital signs, eventually, follows up on the human body. For example, it injects the required chemical.
2) *Battery:* It provides the energy required. If the energy consumption of the sensors is very low, it can use the excess part of the energy from the human body, such as the temperature or vibration. This will allow the engineers to scale down BSU more.
3) *Processor:* It analyzes the data and manages the system.
4) *Antenna:* It is required to format and send the radio frequency signal. Some researchers try to use the human body as a channel of transmission. In this case, an antenna can be removed, and the required power of BSU will become lower.

*C. Types of Sensors*

Body sensor is implanted under the human skin where the electrical properties of the body affect the signal propagations. Those sensors allow the system to measure human body temperature, glucose, or to implement pacemaker. On the other hand, body sensor is integrated into clothes. They are able to be used to monitor heart rate, ECG or respiration rate.

In recent years, with the popularization of wearable sensors and telemedicine, body sensor networks (BSN), which comprise multiple sensor nodes and a coordinator wore on a human body, can collect the personal information of the human body (such as heart rate, blood glucose, and electrocardiogram) by sensor nodes.

The collected information first is delivered to the coordinator, and then is forwarded to a remote server through a network interface for further processing. As shown in Fig 1, vast quantities of the sensor users' personal data are collected by body sensors and recorded by a data centre per second.

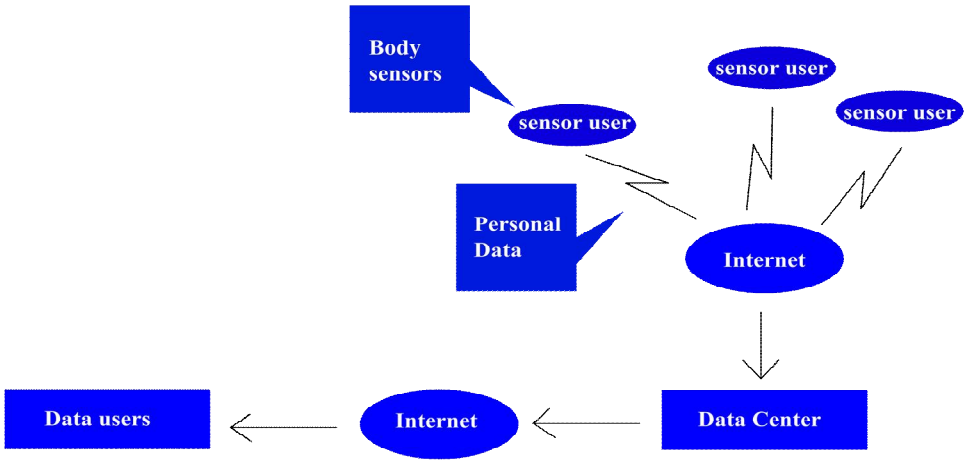



Fig: 1 Body sensor data collection and query service scenario**.**

As a special application of Haptic-technology is body area networks (BANs).They are deployed on the surface of bodies for periodically monitoring physical conditions. In some cases, especially in emergency or health care, security and privacy properties are extremely important, because a slight leakage of sensitive data may cause unpredictable damages. Therefore, extensive studies on privacy preservation have been carried out, which is one of the most critical research topics in BAN.

Usually, data collected, aggregated and transmitted in BANs contain personal and sensitive private information which directly or indirectly reveals the condition of a person.If the data cannot be properly preserved, once exposed to the public, the privacy will be destroyed. Therefore, protecting the privacy of sensitive data is of great importance.

In general, traditional methods for protecting privacy and security of big data in BANs fall into three classes. They are:

*1)* Anonymous techniques
*2)* Privacy protection rules
*3)* Collaborative filtering.

## II. DIFFERENTIAL PRIVACY

The differential privacy provides information about the database while simultaneously ensuring very high levels of privacy. Differential Privacy is a method enabling analysts to extract useful answers from databases containing personal information while offering strong individual privacy protections. It aims to minimize the chances of individual identification while querying the data. The method of differential privacy is shown in fig 2.

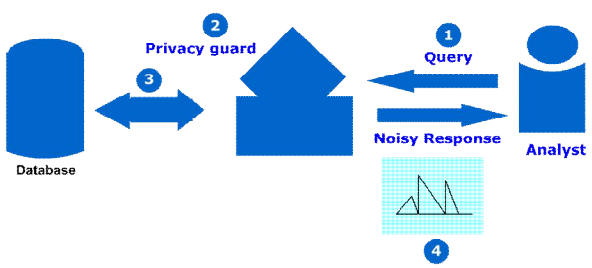



Fig: 2 Working of Differential Privacy

As opposed to anonymization, data is not modified in differential privacy. Users don't have direct access to the database. There is an interface that calculates the results and adds desired inaccuracies. It acts as a firewall. These inaccuracies are large enough that they protect privacy but small enough that the answers provided to analysts and researchers are still useful.

Differential privacy (DP) method prevents unwanted Re-identification and other privacy threats. In this model, Personal information in a large database is not modified. Differential privacy works by inserting an intermediary piece of software between the analyst and the database. The analyst never gets access to the contents of a database. The intermediary acts as a privacy-protecting screen and this serves as privacy guard. Differential privacy aims to provide accurate queries from statistical databases while minimizing the chances of identifying its records. According to this definition, differential privacy is a condition of data release mechanism but not over the dataset itself. This means that for any two datasets that are similar to each other the differential privacy algorithm behaves approximately same on both the datasets. This scheme guarantees that presence or absence of an individual may not affect the final output of the algorithm.

*An Example:* Assume that a hospital has a database of patients with a potentially life-threatening disease. It is shown in Table 1.

Table 1: Hospital Database

| Name | Has Diabetes (X) |
|---|---|
| A | 1 |
| B | 1 |
| C | 0 |
| D | 0 |
| E | 1 |

If we consider the above database of medical records D1 where each record is a pair (Name, X), X is a Boolean denoting whether a person has diabetes or not. Now a malicious user wants to find whether E has diabetes or not and if he knows in which row of E resides. Now the malicious user is only allowed to use a particular form of query Qi that returns the partial sum of first 'i' rows of column X in the database. In order to find E's diabetes status, the adversary executes Q5 (D1) and Q4 (D1) then computes their difference. From the example, Q5 (D1) =3 and Q4 (D1) =2 so their difference is 1. If we construct database D2 by replacing E1 with E0 then this malicious user will be able to distinguish D2 from D1 by computing Q5 – Q4 for each dataset. If the adversary requires receiving values Qi via €- differentially private algorithm then they cannot distinguish between two datasets.

The advantages of differential privacy over anonymization are:

- The original data set is not modified at all. There is no need for suppression or generalization.
- Distortion is added to the results by mathematical calculations based on the type of data, type of questions etc.
- The distortion is added in such a way that value was hidden is useful to analysts.

## III. DIFFERENTIAL PRIVACY IN BAN'S

### *A. Traditional Privacy Methods in BAN's*

This traditional method focused only on data releasing and data mining issues. In this method, once adversary gets successful access to data then the data is completely exposed to the adversary. This traditional method is shown in Fig 3.

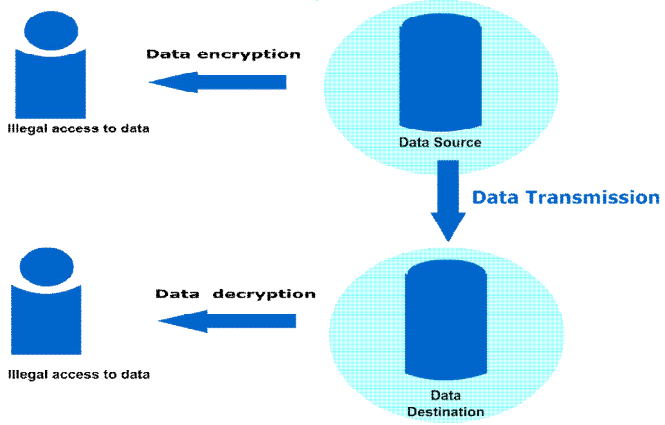



Fig.3 Traditional privacy protections for BAN's

*B. Previous Privacy Methods in BAN's*

In previous methods, raw data is processed and stored in the database. If user queries then the random noise is added to the data and that data is accessed by the user. In this method, if adversary gets to succeed in accessing data in the database then the data is exposed. It is shown in Fig 4.

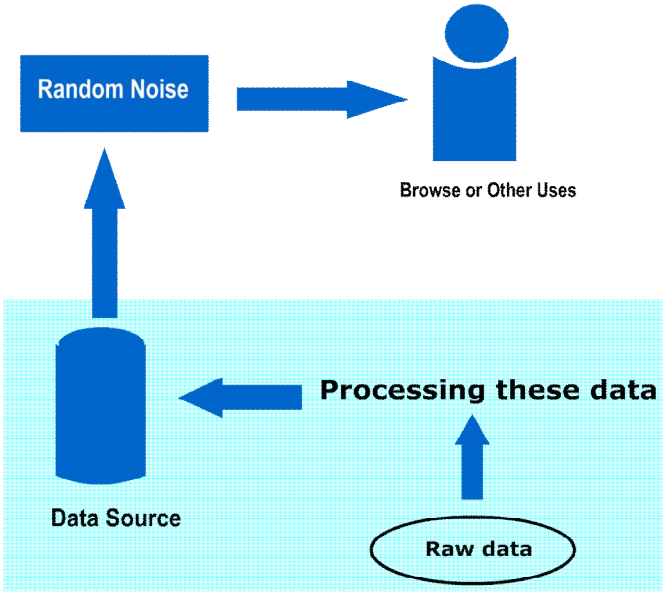



Fig.4 Previous methods

*C. Differential Privacy Method*

This method is our method i.e. differential privacy protection method. In this method we take raw data and process these data during this process we apply differential privacy scheme. In this method adversary can't find the original data if he succeeds in accessing the data source then the complete data can e accessed by the adversary. It is shown in Fig 5.

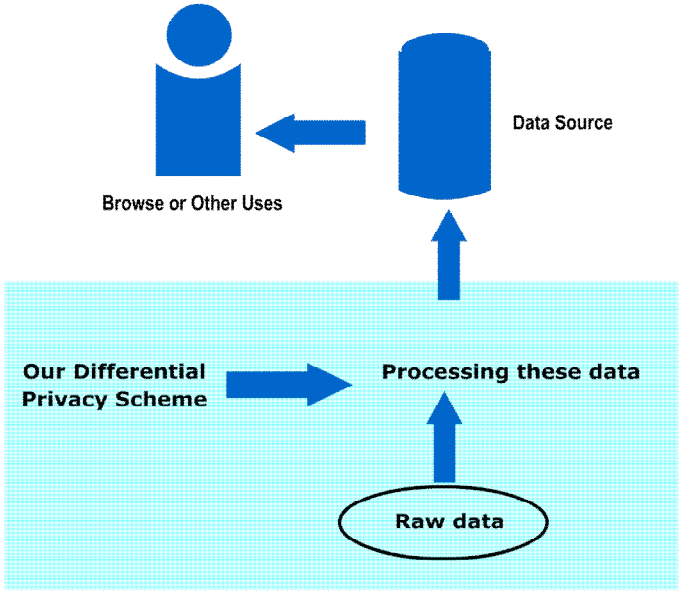


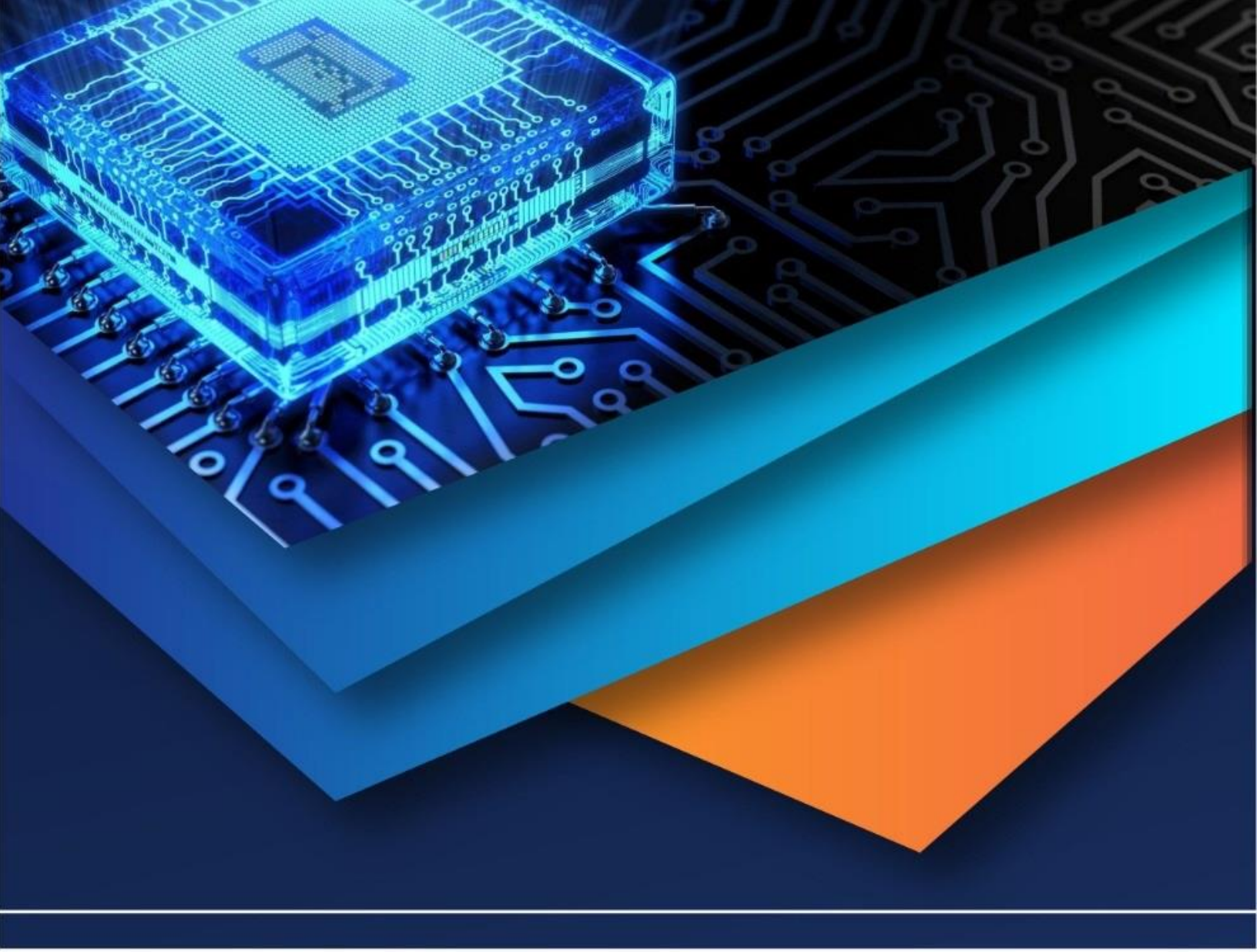

Fig.5 Differential Privacy protection method

## IV. CONCLUSION

In this paper, we proposed a differential privacy protection model for sensitive big data in BANs, which significantly reduces the risk of privacy exposure and greatly ensures the availability of data. Even in the case where the attacker has full knowledge of the background, it can still produce enough interference to data, which can make it unable to find matching.

## REFERENCES

[1] Y., Cayirci, E.:Wireless sensor networks: a survey. Computernetworks 38(4), 393–422 (2002).
[2] Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., Anderson, J.: Wireless sensor networks for habitat monitoring. In: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pp. 88–97. ACM (2002).
[3] Lo, B.P., Thiemjarus, S., King, R., Yang, G.Z.: Body sensor network–a wireless sensor platform for pervasive healthcare monitoring. na (2005).
[4] Lo, B.P., Thiemjarus, S., King, R., Yang, G.Z.: Body sensor network–a wireless sensor platform for pervasive healthcare monitoring. na (2005).
[5] Yang, G.Z.; Yacoub, M. Body Sensor Networks; Springer London: London, UK, 2006.
[6] Erik Karulf, "Body Area Networks (BAN)", April 2008.
[7] Hao, Y., Foster, R.: Wireless body sensor networks for health-monitoring applications. Physiological measurement 29(11), 1–42 (2008).
[8] Li, N., Zhang, N., Das, S.K., Thuraisingham, B.: Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Networks 7(8), 1501–1514 (2009).
[9] Hanson, M.A., Powell Jr, H.C., Barth, A.T., Ringgenberg, K., Calhoun, B.H., Aylor, J.H., Lach, J.: Body area sensor networks: Challenges and opportunities. Computer 1 (1), 58–65 (2009).
[10] Li, N., Zhang, N., Das, S.K., Thuraisingham, B.: Privacy preservation in wireless sensor networks: A state-of-the-art survey. Ad Hoc Networks 7(8), 1501–1514 (2009).
[11] Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: A survey. Computer Networks 54(15), 2688–2710 (2010).
[12] Ann-Kristin Kock, "Medical Body Area Networks", Seminar Kommunikationsstandards in der Medizin, June 2010.
[13] Li, M., Lou, W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wireless Communications 17(1), 51–58 (2010)
[14] Sun, J., Fang, Y., Zhu, X.: Privacy and emergency response in e-healthcare leveraging wireless body sensor networks. IEEE Wireless Communications 17(1), 66–73 (2010)
[15] Dwork, C.: Differential privacy. In: Encyclopedia of Cryptography and Security, pp. 338–340.Springer (2011).
[16] Liu, J., Zhang, Z., Sun, R., Kwak, K.S.: An efficient certificateless remote anonymous authentication scheme for wireless body area networks. In: 2012
[17] IEEE International Conference on Communications (ICC 2012), pp. 3404–3408. IEEE (2012)
[18] Khan, N., Javaid, N., Khan, Z.A., Jaffar, M., Rafiq, U., Bibi, A.: Ubiquitous healthcare in wireless body area networks. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012), pp. 1960–1967. IEEE (2012)
[19] Ullah, S.; Higgins, H.; Braem, B.; Latre, B.; Blondia, C.; Moerman, I.; Saleem, S.; Rahman, Z.; Kwak, K.S. A comprehensive survey of wireless body area networks. J. Med. Syst. 2012.
[20] Antonescu, B., Basagni, S.: Wireless body area networks: challenges, trends and emerging technologies.In: Proceedings of the 8th International Conference on Body Area Networks, pp. 1–7. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2013).
[21] Giannotti, F., Lakshmanan, L.V., Monreale, A., Pedreschi, D., Wang, H.: Privacy-preserving mining of association rules from outsourced transaction databases. IEEE Systems Journal 7(3), 385–395 (2013).
[22] Li, M., Yu, S., Guttman, J.D., Lou,W., Ren, K.: Secure ad hoc trust initialization and key management in wireless body area networks. ACM Transactions on sensor Networks (TOSN) 9(2), 1–35 (2013)
[23] He, D., Chen, C., Chan, S.C., Bu, J., Zhang, P.: Secure and lightweight network admission and transmission protocol for body sensor networks. IEEE Journal of Biomedical and Health Informatics 17(3), 664–674 (2013).
[24] Ma, C.Y., Yau, D.K., Yip, N.K., Rao, N.S.: Privacy vulnerability of published anonymous mobility traces. IEEE/ACM Transactions on Networking 21(3), 720–733 (2013).
[25] Rushanan, M., Rubin, A.D., Kune, D.F., Swanson, C.M.: Sok: Security and privacy in implantable medical devices and body area networks. In: 2014 IEEE Symposium on Security and Privacy (SP 2014), pp. 524–539. IEEE (2014).
[26] Lou, H., Ma, Y., Zhang, F., Liu, M., Shen, W.: Data mining for privacy preserving association rules based on improved mask algorithm. In: Proceedings of the 2014 IEEE 18th International Conference Computer Supported Cooperative Work in Design (CSCWD 2014), pp. 265–270. IEEE (2014).
[27] Lu, Y., Bao, S.D.: Efficient fuzzy vault application in node recognition for securing body sensor networks. In: 2014 IEEE International Conference on Communications (ICC), pp. 3648–3651. IEEE(2014).
[28] James, A.: Optimisation, security, privacy and trust in e-business systems. Journal of Computer and System Sciences 81(6), 941–942 (2015).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY