© February 2016 | IJIRT | Volume 2 Issue 9 | ISSN: 2349-6002

# Reliable Wireless Sensor Network Data Transfer to Mobile Cloud

Sahil J. Meshram[1], Ujwala H. Wanaskar[2]
[1]*PG Student at P.V.P.I.T. Pune, India*
[2]*Asst. Prof. P.V.P.I.T. Pune, India*

***Abstract*— Nowadays, wireless sensor network (WSN) applications have been used in several important areas such as environment monitoring, military, critical infrastructure and construction monitoring, computing and hospitality. As we have receiving data from all this sensors, we use cloud to store data received from all kind of sensors. But due to the limitations of WSNs in terms of storage memory, energy, computation, communication and scalability, efficient management of the large number of WSNs data in these areas is an important issue to deal with. In current scenario, cloud computing is becoming a promising technology to provide a flexible storage and software services in a scalable and virtualized manner at low cost. Therefore, in recent years sensors actively work on cloud to transfer data over mobile. Data transmission is available with the help of Priority-Based Sleep Scheduling (PSS) and Time and Priority Based Selective Data Transmission (TPSDT). But problem occurs when all the data, which is relevant to search has been provided. This will increase time required for transfer as well as energy[1]. To overcome from this problem, I have introduce system called as, "Reliable Wireless Sensor Network Data Transfer to Mobile Cloud". It works on absolute data transmission and mobile cloud. It will provide user specific and asked data instead relevant data. To guarantee the security and efficiency, the data is encrypted before outsourced to cloud, we propose the system with our contribution of adding data security and node security by adding the features of homomorphic encryption algorithm for data security and pair-wise keying for node security.**

***Index Terms*— Wireless sensor networks, mobile cloud computing, integration, usefulness, reliability.**

## I. INTRODUCTION

The WSN is actively use in various domain. It's trend into the various industrial, environmental, and commercial fields. A typical sensor network may consist of a number of sensor nodes acting upon together to monitor a region, which fetches data about the surroundings. A WSN contains spatially distributed self-regulated sensors that can cooperatively monitor the environmental conditions, like sound, temperature, pressure, motion, vibration, pollution, and so forth [1]. Where node in a sensor network is loaded with wireless communication device (like a radio transceiver or some other), a small microcontroller and an energy source most often cells/battery. The nodes of sensor network are comes with cooperative capabilities, which are usually deployed in a random manner. Sensing, processing, and communicating are three base parts of sensors. Camera sensor, accelerometer sensor, thermal sensor, microphone sensor and many other devices categorized under sensor devices.

we propose the system with our contribution of adding data security and node security by adding the features of homomorphic encryption algorithm for data security and pair-wise keying for node security.

We propose an efficient system for preventing location leaks in Sensor Networks and also it ensures the privacy-preserving scheme against traffic analysis and flow tracing.

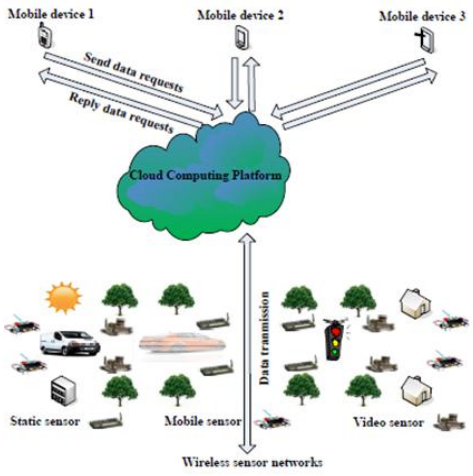


Figure 1: WSN-MCC Integration framework

Mobile sinks (MSs) are vital in many wireless sensor network (WSN) applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. However, in sensor networks that make use

of the existing key pre distribution schemes for pair-wise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge. Thus introducing the data security and node security algorithm in existing system makes the system more efficient and accurate.

## II. PROBLEM STATEMENT

WSN-MCC integration with Security Features for increased secure computing. we propose the system with our contribution of adding data security and node security by adding the features of homomorphic encryption algorithm for data security and pair-wise keying for node security. We propose an efficient system for preventing location leaks in Sensor Networks and also it ensures the privacy-preserving scheme against traffic analysis and flow tracing. With the faster homomorphic encryption algorithm technique, the proposed scheme offers two significant privacy preserving features, packet flow untraceability and message content confidentiality, which can efficiently thwart traffic analysis/flow tracing attacks. Moreover, with homomorphic encryption, the proposed scheme keeps the essence of random linear network coding, and each sink can recover the source messages by inverting with a very high probability.

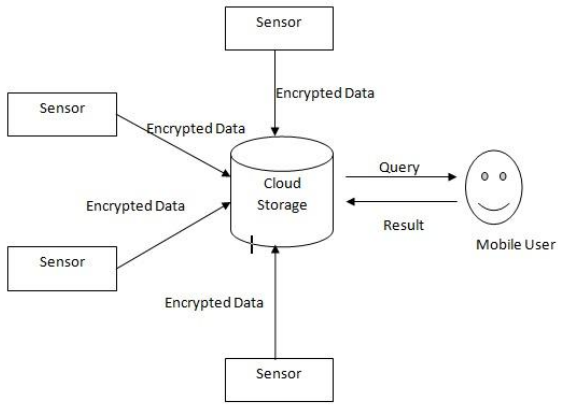


Figure 2: WSN-MCC integration with Security

The quantitative analysis and simulative evaluation on privacy enhancement and computational overhead demonstrate the effectiveness and efficiency of the proposed scheme. Mobile sinks (MSs) are vital in many wireless sensor network (WSN) applications for efficient data accumulation, localized sensor reprogramming, and for distinguishing and revoking compromised sensors. However, in sensor networks that make use of the existing key pre distribution schemes for pair-wise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge. Thus introducing the data security and node security algorithm in existing system makes the system more efficient and accurate.

## III. LITERATURE SURVEY

S.K. Dash, S. Mohapatra, P.K. Pattnaik , The communication among sensor nodes using Internet is a challenging task since sensor nodes contain limited band width, memory and small size batteries. The issues of storage capacity may be overcome by widely used cloud computing technique. some issues of cloud computing & sensor network. To develop a new protocol in sensor network, the specific application oriented scenarios are of important consideration. some typical applications of Sensor Network using Cloud computing as backbone. Since Cloud computing provides plenty of application, platforms and infrastructure over the Internet; it may combined with Sensor network in the application areas such as environmental monitoring, weather forecasting, transportation business, healthcare, military application etc. Bringing various WSNs deployed for different applications under one roof and looking it as a single virtual WSN entity through cloud computing infrastructure is novel [2].

Sukanya C.M, Priya K.V, Vince Paul, Mr.Sankaranarayanan P.N proposes presents a comprehensive survey on the sensory data processing framework to integrate wireless sensor networks with mobile cloud. It also describes about the communication and data management issues in mobile sensor networks. Describes the concept of wireless sensor networks and mobile cloud computing. a framework to process the sensory data collected by the sensors, before transmitting the sensory data to mobile users in a fast, reliable, and secure manner. This framework includes data traffic monitoring, filtering, prediction, compression, and decompression capabilities are incorporated in the sensor gateway and the cloud gateway. Data encryption and decryption techniques are applied in the cloud, mobile devices, and sensor and cloud gateways to increase capacity. Due to the advanced capabilities and high performance of the proposed framework the mobile users can securely obtain their desired sensory data faster [3].

Subhash Dhar Dwivedi, Praveen Kaushik In wireless sensor network most of the devices operate on batteries. These devices or nodes have limited amount of initial energy that are consumed at different rates, depending on the power level and intended receiver. In sleep scheduling algorithms most of thenodes are put to sleep to conserve energy and increase network life time . There are to main approaches to sleep scheduling i) random ii) synchronized. Main purpose of any sleep scheduling algorithm is to maintain network connectivity. A novel approach for sleep scheduling of sensor nodes using a tree and an energy aware routing protocol which is integrated with the proposed sleep scheduling scheme. The tree is rooted at the sink node .The tree is periodically reconstructed considering the remaining energy of each node with a view to balance energy consumption of nodes, and remove any failed nodes from the tree. The proposed approach also considerably reduces average energy consumption rate of each node as we are able to put more number of nodes to sleep in comparison to other approaches such as GSP, which incorporates sleep scheduling using random approach[4].

Payal V. Parmar, Shraddha B. Padhar, Rutvij H. Jhaveri, The homomorphic encryption and the various encryption algorithms as per the properties of the homomorphic encryption; Paillier can be used for preserving the additive property of homomorphic encryption while ElGamal and RSA can be used for multiplicative property. This paper can be useful for those who are wishing to carry out research in the direction of the cryptographic algorithms used for homomorphic encryption. This survey can be helpful to know which and how various cryptographic algorithms are being used for applying homomorphic encryption for privacy preservation. used for mixed homomorphic encryption property. At last the comparison of all homomorphic encryption algorithms and schemes is done which may help to extend current research techniques[5].

## IV. CONCLUSION

WSN-MCC to data transfer with reliable and usefulness .focused on WSN-MCC integration by incorporating the ubiquitous data gathering ability of WSN and the powerful data storage and data processing capabilities of MCC. Support WSN-MCC integration applications that need more useful data offered reliably from the WSN to the cloud, we have identified the critical issues that impede the usefulness of sensory data and reliability of WSN, and proposed a novel WSN-MCC integration scheme named TPSS to address some of these issues. 1) TPSDT for WSN gateway to selectively transmit sensory data that are more useful to the cloud, considering the time and priority features of the data requested by the mobile user.

2)PSS algorithm for WSN to save energy consumption so that it can gather and transmit data more reliably. Both analytical and experimental results regarding TPSS have been presented to demonstrate the effectiveness of TPSS in improving the usefulness of sensory data and reliability of WSN for WSN-MCC integration. Security Features for increased secure computing. In this project we propose the system with our contribution of adding data security and node security by adding the features of homomorphic encryption algorithm for data security and pair-wise keying for node security. We propose an efficient system for preventing location leaks in Sensor Networks and also it ensures the privacy-preserving scheme against traffic analysis and flow tracing.

## REFERENCES

[1] Chunsheng Zhu, Student Member, IEEE, Zhengguo Sheng *"Towards Offering More Useful Data Reliably to Mobile Cloud from Wireless Sensor Network"* IEEETransactions On Emerging Topics In Computing, Vol. 03, October 2014.

[2] Sanjit Kumar Dash, Subasish Mohapatra , Prasant Kumar Pattnaik " *A Survey on Applications of Wireless Sensor Network Using Cloud Computing" International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004)* 50 *Volume 1, Issue 4, December 2010*

[3] Sukanya C.M, Priya K.V, Vince Paul" *Integration of Wireless Sensor Networks and Mobile Cloud"* Sukanya C.M et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015

[4] Subhash Dhar Dwivedi, Praveen Kaushik *"Energy*

*Efficient Routing Algorithm with sleep scheduling in*
*Wireless Sensor Network"* Subhash Dhar Dwivedi et al, / (IJCSIT)
International Journal of Computer Science and Information Technologies,
Vol. 3 (3) , 2012.

[5] Payal V. Parmar, Shraddha B. Padhar, Niyatee I. Bhatt" *Survey of Various Homomorphic Encryption*
*algorithms and Schemes"* International Journal of Computer
Applications (0975 – 8887) Volume 91 – No.8, April 2014