Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

Private and Secure Data Transmission and Analysis for Wireless Networks

Raghavendra D. Krushnaji[1], Pooja Sonkambale.[2], Priyanka Shikare[3], Seema More[4], and Dhiraj Pawar[5]

[1]*Dept. of Computer Engineering*

Imperial College of Engineering & Research, Pune, India

rdkrushnaji@gmail.com

[2,3,4,5]*Dept. of Computer Engineering*

Imperial College of Engineering & Research, Pune, India

Abstract **— In recent years the use of internet is widely increased. We all uses internet in our day to day life. Internet become a part of our life and we are using not only wired but also wireless devices/gadgets to use an internet. Most of the people use internet for data transmission. The data which we are transferring can be private or sensitive data related to an individual person. While we transfer data there can be many attack made by outsider or insider. A lot of work has been done to secure sensitive information. The new approaches are design to prevent these attacks. Wireless networks are generally less secure. If the network hasn' t been set up to be password protected there are problems with bandwidth stealing. In wireless systems, information is also less secure and can be easier to hack into. This paper contains a brief study of various strategies used to securely share the bandwidth as well as sensitive information.**

I. INTRODUCTION

Data transmission is the process of sending digital or analog data on communication medium from one computer to another, network or devices etc. Data transmission can be analog or digital but mainly used for digital data. It works when user wants to send some data or files to one or more recipient. The digital data on the source device is in the form of digital bit stream. This data stream then transfer through communication media such as physical copper wires or wireless network to destination device. Privacy needed whenever the private information of a person or sensitive information related to a person is collected, stored, used and then deleted in digital form or in another form. Data privacy issue may be arise when the information can be leak from a wide range of sources such as hospital record, college record, Financial institutions and transactions etc. The challenge of data privacy is to protect the data of individual. Data security is design to address this issue. The laws related to data Protection are changing according to the time. However the new technologies are design to protect the data the laws related protocols also changes.

Difference between wired and wireless network as follows: The development of Privacy Protection for organizational database was motivated by business applications; today such networks are used in many organizational, educational and consumer applications, such as business process monitoring and control, and so on [1]. What has received less attention,

however, is the critical privacy concern on information being collected, transmitted, and analyzed. Such private information may include payload data transmitted through the network to a centralized data processing server. Our objective is: Protect the user data during transmission. To achieve users data collection, transmission, processing and presentation has become a critical issue in many applications, in which a variety of wireless sensor nodes and terminal devices has important roles in network data aggregation and communications[2].

II. LITERATURE REVIEW

A. Sharemind: a framework for fast privacy-preserving Computations Gathering and processing sensitive data is a difficult task. In fact, there is no common recipe for building the necessary information systems. In this paper, they present a provably secure and efficient general-purpose computation system to address this problem. The solution " SHAREMIND" is a virtual machine for privacy-preserving data processing that relies on share computing techniques. This is a standard way for securely evaluating functions in a multi-party computation environment. The novelty of our solution is in the choice of the secret sharing scheme and the design of the protocol suite. The protocols

All Rights Reserved, @IJAREST-2018

of SHAREMIND are information-theoretically secure in the honest-but-curious model with three computing participants. Although the honest-but-curious model does not tolerate malicious participants, it still provides significantly increased privacy preservation when compared to standard centralized databases.

B. Real-Time and Secure Wireless Health Monitoring[9] In this paper a framework for a wireless health monitoring system using wireless networks such as ZigBee. Vital signals are collected and processed using a 3-tiered architecture. The first stage is the mobile device carried on the body that runs a number of wired and wireless probes. This device is also designed to perform some basic processing such as the heart rate and fatal failure detection. At the second stage, further processing is performed by a local server using the raw data transmitted by the mobile device continuously. The raw data is also stored at this server. The processed data as well as the analysis results are then transmitted to the service provider center for diagnostic reviews as well as storage. The main advantages of the proposed framework are:

(1) the ability to detect signals wirelessly within a body sensor network (BSN),
(2) low-power and reliable data transmission through ZigBee network nodes,
(3) secure transmission of medical data over BSN,
(4) efficient channel allocation for medical data transmission over wireless networks, and
(5) optimized analysis of data using an adaptive architecture that maximizes the utility of processing and computational capacity at each platform.

C. A Novel and Lightweight System to Secure Wireless Sensor Networks[11] Wireless sensor networks (MSNs) are a key enabling technology in e-health-care that allows the data of a user vital body parameters to be collected by the wearable or implantable bio-sensors. However, the security and privacy protection of the collected data is a major unsolved issue, with challenges coming from the stringent resource constraints of MSN devices, and the high demand for both security/privacy and practicality. In this paper, we propose a lightweight and secure system for MSNs. The system employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and fine- grained data access control. Furthermore, we extend the sys- tem to provide backward secrecy and privacy preservation. Our system only requires symmetric-key encryption/ decryption and hash operations and is thus suitable for the low-power sensor nodes. This paper also reports the experimental results of the proposed system in a network of resource-limited motes and laptop PCs, which show its efficiency in practice. To the best of our knowledge, this is the first secure data transmission and access control system for MSNs until now.

D. Pervasive, Secure Access to a Hierarchical Sensor-based Health-care Monitoring Architecture in Wireless Heteroge- neous Networks(2009)[7]

This study presents a health-care monitoring architecture coupled with wearable sensor systems and an environmental sensor network for monitoring elderly or chronic patients in their residence. The wearable sensor system, built into a fabric belt, consists of various medical sensors that collect a timely set of physiological health indicators transmitted via low energy wireless communication to mobile comput- ing devices. Three application scenarios are implemented using the proposed network architecture. The group-based data collection and data transmission using the ad hoc mode promote outpatient health-care services for only one medical staff member assigned to a set of patients. Adaptive security issues for data transmission are performed based on different wireless capabilities. This study also presents a monitoring application prototype for capturing sensor data from wireless sensor nodes. The implemented schemes were verified as performing efficiently and rapidly in the proposed network architecture.

G. Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems against False Data Injection Attacks and Jamming Attacks[15] This paper is concerned with the problem of joint distributed attack detection and distributed secure estimation for a networked cyber-physical system under physical and cyber attacks. The system is monitored by a wireless sensor network in which a group of sensors is spatially distributed and the sensors measurements are broadcast to remote estimators via a wireless network medium. The distributed attack detection and secure estimation problem for a CPS over a WSN in the presence of two types of malicious attacks To tackle the random jamming attacks. The refined measurement output model based on compensated measurements has been proposed and resilient estimators are delicately constructed.

H. Achieving Private, Scalable, and Precise Data Collection in Wireless Sensor Networks[17] Remote Sensor Networks (WSN) turn out to be progressively well known to gather information over an extensive zone. Given the gathered informational index, the system supervisor can extricate different sorts of total measurements from the set to describe the physical space. On the accumulation of the information, three prerequisites ought to be forced: (1) Privacy: as sensor hubs are source restricted and regularly conveyed in an open situation, the detected information experiences the ill effects of protection vulnerabilities. Secure component ought to be given to ensure information protection, (2) Communication productivity: gathering information from vast scale sensor organizes regularly includes extensive volume information age

All Rights Reserved, @IJAREST-2018

and transmission, which may rapidly expend the vitality of the WSN. To delay the lifetimes of the sensor hubs, the detected information ought to be transmitted in lightweight way, (3) Accuracy: the detected information ought to be recuperated precisely at the base station (BS) with the goal that the chief can control them unreservedly to accomplish any exact total measurement he favors. To fulfill these prerequisites, we propose two novel security protecting information accumulation plans in light of compressive detecting strategies. Our plans address the security, correspondence proficiency and precision issues all the while. Definite hypothetical examination and reproduction comes about affirm the elite of the proposed plans.

I. Efficient aggregation of encrypted data in wireless sensor networks[17] Remote sensor systems (WSNs) are specially appointed systems made out of little gadgets with restricted calculation and vitality limits. For such gadgets, information transmission is an exceptionally vitality devouring operation. It in this manner winds up plainly basic to the lifetime of a WSN to limit the quantity of bits sent by every gadget. One surely understood approach is to total sensor information (e.g., by including) along the way from sensors to the sink. Accumulation turns out to be particularly testing if end-toend protection among sensors and the sink is required. In this paper, we propose a straightforward and provably secure additively homomorphic stream figure that permits proficient accumulation of encoded information. The new figure just uses secluded augmentations (with little moduli) and is in this manner exceptionally appropriate for CPU-compelled gadgets. We demonstrate that total in view of this figure can be utilized to productively process measurable esteems, for example, mean, fluctuation and standard deviation of detected information, while accomplishing critical transfer speed pick up.

J. A study of the energy consumption characteristics of cryptographic algorithms and security protocols[18] Security is turning into a regular worry for an extensive variety of electronic frameworks that control, impart, and store touchy information. A critical and developing classification of such electronic frameworks is battery-fueled portable machines, for example, individual advanced partners (PDAs) and PDAs, which are seriously compelled in the assets they have, to be specific, processor, battery, and memory. This work concentrates on one imperative requirement of such gadgets battery life-and analyzes how it is affected by the utilization of different security instruments. In this paper, we first present an extensive examination of the vital necessities of an extensive variety of cryptographic calculations that frame the building squares of security systems, for example, security conventions. We at that point think about the vitality utilization prerequisites of the most well known transport-layer security convention: Secure Sockets Layer (SSL). We research the effect of different parameters at the convention level, (for example, figure suites, confirmation components, and exchange sizes, and so on.) and the cryptographic calculation level (figure modes, quality) on the general vitality utilization for secure information exchanges. As far as anyone is concerned, this is the principal far-reaching examination of the vitality prerequisites of SSL. For our examinations, we have built up an estimation based test testbed that comprises of an iPAQ PDA associated with a remote neighborhood (LAN) and running Linux, a PCbased information obtaining framework for continuous current estimation, the OpenSSL usage of the SSL convention, and parameterizable SSL customer and server test programs. In view of our outcomes, we additionally talk about different open doors for acknowledging vitality effective executions of security conventions. We accept such examinations to be an essential initial move toward tending to the difficulties of vitality effective security for battery-obliged frameworks.

III. TECHNIQUES USED

1) SHAREMIND: It is a virtual machine for privacy-preserving process that depends on share computing techniques. Typically often a typical suggests that for firmly evaluating functions in a multi-party computation surroundings. The novelty of answer is inside the selection of the key sharing theme and therefore the style of the protocol suite. this concept have created many smart decisions to make large-scale share computing possible in observe. The protocols of SHAREMIND are information-theoretically secure inside the honest-but-curious model with three computing participants. though the honest-but-curious model does not tolerate malicious participants, it still provides significantly enlarged privacy preservation once place next to plain centralized databases.

2) Pailler Cryptography: This is an encryption scheme that may be used to conceal info, with many interesting properties. These properties, once creatively applied, enable the Paillier Cryptosystem to be used in ways in which alternative cryptographic systems merely can’ t be used. This document can discover though the Paillier Cryptosystem works, however these property arise, and a way in which the system will be employed in a true world scenario as a results of these properties.

All Rights Reserved, @IJAREST-2018

IV. CONCLUSION

In this paper, we have investigated the security and privacy related issues in wireless networks. We also studied the different mechanisms like SHAREMIND and Pailler Cryptography through which the security in wireless networks can be enhanced.

REFERENCES

[1] Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson, Privacy Protection for Wireless Medical Sensor Data, in proc. IEEE Transactions on Dependable and Secure Computing, 2015.

[2] Haiping Huang, Member, IEEE, Tianhe Gong, Ning Ye, Ruchuan Wang and Yi Dou, Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System, Year: 2017, Volume: 13, Issue: 3

[3] Bogdanov, S. LaurSharemind, A Framework for Fast Privacy-Preserving Computations, in Proc. ESORICS08, pages 192-206D.

[4] C.Gayathri, D.Sathya, Protection of Security and Privacy for Medical Data in Wireless Medical Sensors Networks , IJARSE, Vol. No.4, Special Issue (01), March 2015.

[5] William Stallings, Cryptography And Network Security, book edition 5th, 6th ,7th.

[6] Wood A. , Virone G. , Doan T. , Cao Q. , Selavo L. , Wu Y. , Fang L. , He Z. , Lin S. , Stankovic J. , ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring , Technical Report CS-2006-01, Department of Computer Science, University of Virginia: Charlottesville, VA, USA, 2006.

[7] Chen, B.R. , Peterson, G. , Mainland, G. , Welsh M. ,LiveNet: Using Passive Monitoring to Reconstruct Sensor Network Dynamics, In Proceedings of the 4th IEEE International Conference on Distributed Computing in Sensor System (DCOSS08), Santorini Island, Greece, 1114 June 2008.

[8] Dimitriou T. ,Loannis K. ,Security Issues in Biomedical Wireless Sensor Networks, In Proceedings of 1st International Symposium on Applied Sciences on Biomedical and Communication Technologies (ISABEL08), Aalborg, Denmark, 2528 October 200

All Rights Reserved, @IJAREST-2018