Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 01, January -2019

PRIVACY PROTECTION FOR STUDENT DATA USING PAILLERS CRYPTOSYSTEM

Payal Mane[1] Mugdha Talele [2]Kaustubh Warke [3]

Abstract: *Student applications are considered as promising fields privacy protection of student data, where students can be monitored using privacy protection of student data. Current student research trends focus on student reliable communication, student mobility, and energy-efficient routing, as a few examples. However, deploying new technologies in student applications without considering security makes student privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of student applications, especially in the case of student privacy, if the student has an embarrassing disease. This project discusses the security and privacy issues in student application using privacy protection of student data. We highlight some popular student projects using privacy protection of student data, and discuss their security the existing systems solutions can simply protect the student data during transmission, but cannot protect the inside attack where the administrator of the student database reveals the sensitive student data. So we are proposing a approach to prevent the inside attack by using multiple data servers to store student data. The main contribution of this paper is to distribute student's data securely in multiple data servers and performing the Paillier cryptosystems to perform statistical analysis on the student data without compromising the student's privacy.*

***Keywords*:** *student application, student data privacy, Paillier encryption.*

I. INTRODUCTION

A privacy protection of student is a network to monitor physical or environmental conditions such as temperature, sound, pressure, etc. The development of privacy protection of student networks was motivated by air pollution monitoring, water quality monitoring, land side detection, forest fire detection, habitat monitoring and so on. Though there are many applications in privacy protection of student network domain, human healthcare applications takes the major role. In human healthcare, sensors are used to monitor the students' health status such as temperature level, sugar level, heart beat rate, blood pressure. For instance, if the student's sugar level is monitored 10 times per day then the data is updated in the database which is present in the local server. Likewise the values for blood pressure, heart beat, and temperature are also noted at regular intervals. There are many security issues such as data stealing, stealing and updating, storing the wrong values. Suppose if the intruder is trying to hack the student details, there are many chances for the misuse of data which may lead to severe consequences. The data can also be modified by the hackers due to lack of security. The treatment prescribed by the doctors can be hacked which may even lead to death of the students. student are the victims because of the above issues. To prevent these issues, the intrusion detection system is proposed. An intrusion detection system is a system used to check the malicious activities and produces electronic reports to a management station. It consists of Paillier algorithmkey cryptosystems. The algorithm isused to encrypt the student details before storing it in the database and perform decryption when needed by the admin.

Algorithm:

A) Paillier Public-Key Cryptosystem:

It is composed of key generation, encryption and decryption algorithms as follows.

1)Key generation

The key generation algorithm works as follows.

- Choose two large prime numbers p and q randomly and independently of each other such that

$$\gcd\big(pq,(p-1)(q-1)\big)=1$$

- Compute

$$N=pq,\lambda=lcm(p-1,q-1)$$

Where lcm stands for the least common multiple.

- Select random integer g where g ∈ and ensure N divides the order of g by checking the existence of the following modular multiplicative inverse:

$$\mu = \left(L\left(g^{\lambda}(mod N^2)\right)\right)^{-1}(mod\ N)$$

where function L is defined as

$$L(u) = \frac{u-1}{N}$$

Note that the notation a/b does not denote the modular multiplication of a times the modular multiplicative inverse of b but rather the quotient of a divided by b.

The public (encryption) key pk is (N,g).
The private (decryption) key sk is (λ,μ).

If using p,q of equivalent length, one can simply choose

$$g = N + 1, \lambda = \varphi(N)^{-1}(mod\ N)$$

where N = pq and

2)Encryption:

The encryption algorithm works as follows.

- Let m be a message to encrypt, where m ∈
- Select random r where r ∈
- Compute ciphertext as:

$$C = g^m . r^N (mod\ N^2)$$

3)Decryption:

The decryption algorithm works as follows.

- Let c be the ciphertext to decrypt, where the ciphertext c∈.
- Compute the plaintext message as:

$$m = \left(c^{\lambda}(mod\ N^2)\right).\mu(mod\ N)$$

4)Homomorphic Properties

A notable feature of the Paillier cryptosystem is its homomorphic properties. Given two ciphertexts

$$E(m_1, pk) = g^{m1} r_1^N (mod\ N^2)$$
$$E(m_2, pk) = g^{m2} r_2^N (mod\ N^2)$$

where r1,r2 are randomly chosen for ,we have the following homomorphic properties.

$$D\left(E(m_1, pk_1).E(m_2, pk_2)\right) = m_1 + m_2 (mod\ N)$$

The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$$D(E(m_1, pk_1).g^{m2}) = m_1 + m_2 (mod\ N)$$

An encrypted plaintext raised to a constant k will decrypt to the product of the plaintext and the constant,

$$D(E(m_1, pk_1)^k) = km_1 (mod\ N)$$

However, given the Paillier encryptions of two messages, there is no known way to compute an encryption of the product of these messages without knowing the private key.

II. LITERATURE SURVEY

1. Sharemind: a framework for fast privacy-preserving Computations (2008).
Authors: Dan Bogdanov, Sven Laur1, and Gregorian calendar month Willemson
Description:
Gathering and process sensitive knowledge may be a tough task. In fact, thereis no common direction for building the required info systems. during this paper, we gift a incontrovertibly secure and economical general computation systemto address this downside. Our solution—SHAREMIND—is a virtual machinefor privacy-preserving processing that depends on share computing techniques. This is a customary manner for firmly evaluating functions in a very multi-party computation atmosphere. The novelty of our resolution is within the alternative of the key sharing scheme and also the style of the protocol suite. we've created several sensible decisions to create large-scale share computing possible in follow. The protocols of SHAREMIND square measure information-theoretically secure within the honest-but-curious model with 3 computing participants. though the honest-but-curious model does not tolerate malicious participants, it still provides considerably increased privacy preservation compared to plain centralised databases.

2. Real-time and Secure Wireless Health Monitoring
Authers: S. Dagtas, G. Pekhteryev, Z. S¸ahinoglu, H. Cam, and N. Challa
Description:
We gift a framework for a wireless health observance system exploitation wireless networks like ZigBee. important signals square measure collected and processed employing a 3-tiered design. the primary stage is that the mobile device carried on the body that runs variety of wired and wireless probes. This device is additionally designed to perform some basic process like the guts rate and fatal failure detection. Atthe second stage, any process is performed by an area server exploitation the information transmitted by the mobile device contineously. The information is additionally hold on at this server. The processed knowledge yet because the analysis results square measure then transmitted to the service supplier center for diagnostic reviews yet as storage. the most benefits of the projected framework square measure (1) the power to discover signals wirelessly inside a body sensing element network (BSN), (2) low-power and reliable knowledge transmission through Zig Bee network nodes, (3) secure transmission of medical knowledge over BSN, (4) economical channel allocation for medical knowledge transmission over wireless networks, Associate in Nursingd (5) optimized analysis of information exploitation an adjustive design that maximizes the utility of processing and process capability at every platform.

3. A novel and lightweight System to Secure Wireless Medical sensor Networks
Authors: Daojing He, Sammy Chanand Shaohua Tang.
Description:
Wireless medical sensing element networks (MSNs) square measure a key enabling technology in e-healthcare that enables the information of patient's important body parameters to be collected by the wearable or implantable biosensors. However, the protection and privacy protection of the collected knowledge may be a major unresolved issue, with challenges coming back from the demanding resource constraints of MSN devices, and the high demand for each security/privacy and utility. during this paper, we have a tendency to propose a light-weight and secure system for MSNs. The system employs hash-chain primarily based key change mechanism and proxy-protected signature technique to attain economical secure transmission and fine-grained knowledge access management. any additional, we have a tendency to extend the system to supply backward secrecy and privacy preservation. Our system solely needs symmetric-key encryption/decryption and hash operations and is therefore appropriate for the low-power sensing element nodes. This paper conjointly reports the experimental results of the projected system in a very network of resource-limited motes and laptop computer PCs, that show its potency in follow. To the best of our data, this is often the primary secure knowledge transmission and access system for MSNs yet.

4. Pervasive, Secure Access to a Hierarchical Sensor-based aid observance design in Wireless Heterogeneous Networks
Authors: Y.M. Huang, M.Y. Hsieh, H.C. Chao, S.H. Hung, and J.H. Park.
Description:
This study presents a aid observance design including wearable sensing element systems Associate in Nursingd an environmental sensor network for observance senior or chronic patients in their residence. The wearable sensing element system, built into a material belt, consists of assorted medical sensors that collecta timely set of physiological health indicators transmitted vialow energy wireless communication to mobile computing devices. Three application situations square measure enforced exploitation the projected specification. The group-based knowledge assortment and knowledge transmission exploitation the unintended mode promote patient aid services for less than one medical employee assigned to aset of patients. adjustive security problems for knowledge transmission are performed supported completely different wireless capabilities. This study alsopresents a observance application model for capturing sensing element data from wireless sensor nodes. The enforced schemes wereverified as playacting expeditiously and apace within the proposed network design.

III. EXISTING SYSTEM

The security may be a overriding demand of care applications, particularly within the case of patient privacy, if the patient has AN embarrassing malady. This project discusses the safety and privacy problems in care application victimization WMSNs. we tend to highlight some widespread care comes victimization wireless medical device networks, and discuss their security the prevailing systems solutions will merely shield the patient knowledge throughout transmission, however cannot shield the within attack wherever the administrator of the patient info reveals the sensitive patient knowledge.

3.1 Disadvantages of Existing System

1. Less secure.
2. Cannot protect inside attacker.
3. If any hacker get data from one DB server then whole data will be get to hacker.

IV. PROPOSED SYSTEM

.

To prevent the student information from the within attacks, we tend to propose a brand new information assortment protocol, wherever a device splits the sensitive student information into 3 parts in line with a random range generator supported hash perform and sends them to 3 servers, respective, via securechannels.To keep the privacy of the student information in information access, we tend to propose a brand new information access protocol on the idea of the Paillier cryptosystem. The protocol permits the user to access the student information while not revealing it to any information server. To preserve the privacy of the student information in applied mathematics analysis, we tend to propose some new privacy-preserving applied mathematics analysis protocol on the idea of the Paillier cryptosystems. These protocols permit the user to perform applied mathematics analysis on the student information while not compromising the student information privacy.

4.1 Advantages of Proposed System

1. Practical approach to prevent the inside attack by securely distributing the patient data in multiple data servers.

2. Employing the Paillier cryptosystems to perform statistical analysis on the patient data without compromising the patients' privacy.

3. In Proposed system, Due to secured distributed database architecture we can achieve data storage & data analysis security.

4. Proposed data retrieval technique allow to retrieve the data compromised server(s)

V. SYSTEM ARCHITECTURE

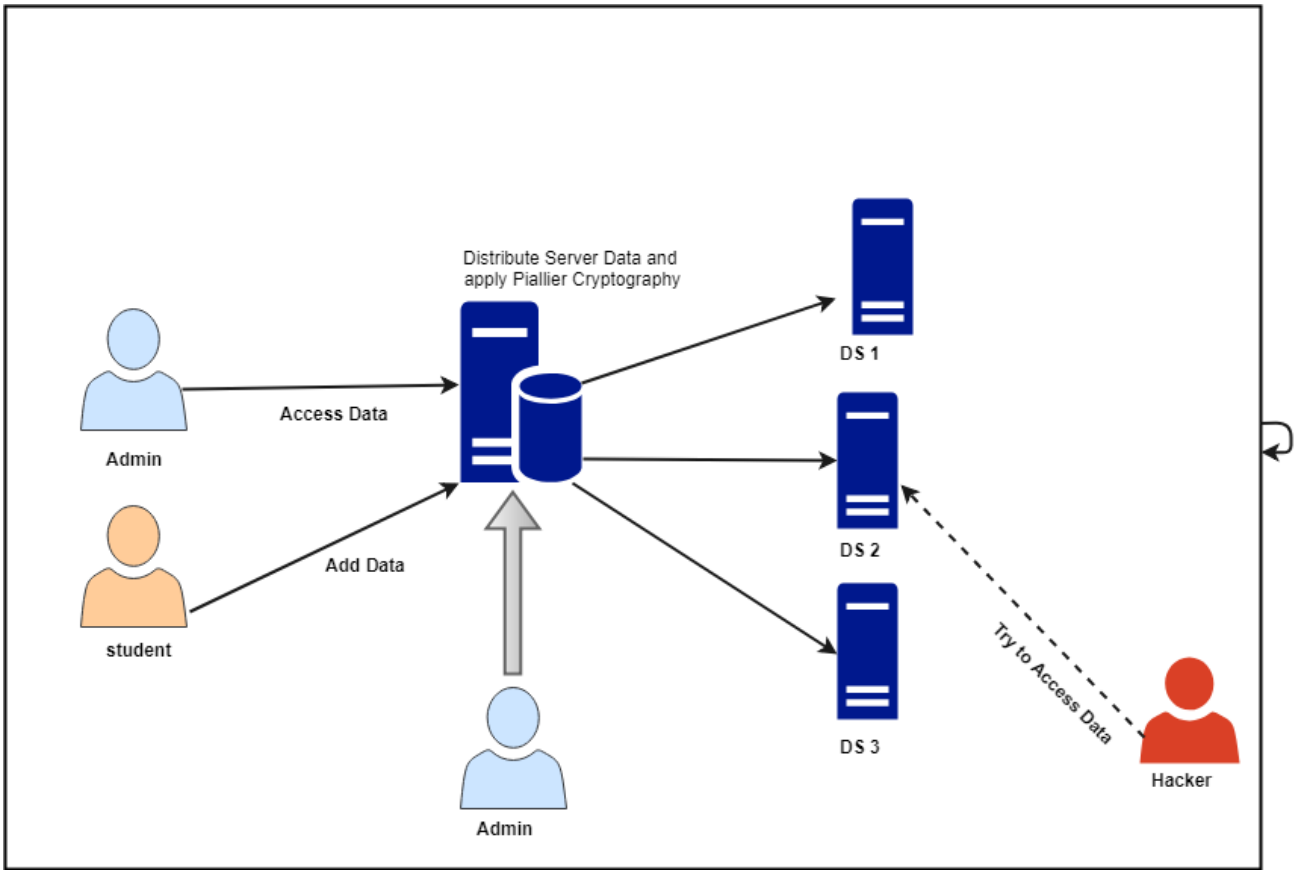

Figure 1. Proposed System Architecture

VI. CONCLUSION

We have investigated the protection and privacy issues within the student sensor data collection storage and queries and presented a complete answer for privacy-preserving student sensing element net-work through the ad-hoc network. to stay the privacy of the patient data, we tend to proposed a replacement knowledge collection protocol that splits the patient knowledge into 3 numbers and stores them in 3 knowledge servers, severally. As long collectively data server isn't compromised, the privacy of the patient knowledge are often preserved. For the legitimate user e.g. Dr. to access the coed knowledge, we tend to projected AN access management protocol, wherever 3 data servers get together to produce the user with the student data, however don't recognize what it's. just in case any 2 of 3 servers square measure compromised the projected system provides a proxy based knowledge retrieval system.

REFERENCES

[1] Yi, Xun, et al. ”Privacy Protection for Wireless Medical Sensor Data.” IEEE Transactions on Dependable and Secure Computing 13.3 (2016): 369-380.
[2] X. Yi, J. Willemson, F. Nat-Abdesselam. Privacy-Preserving Wireless Medical Sensor Net-work. In Proc. TrustCom13, pages 118-125, 2013.
[3] D. He, S. Chan and S. Tang. A Novel and Lightweight System to Secure Wireless Medical Sensor Networks. IEEE Journal of Biomedical and Health Informatics, 18 (1): 316-326, 2014.
[4] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchi-cal Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 27: 400-411, 2009.
[5] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9: 6273-6297, 2009.

