AKHIL BHARATIYA MARATHA SHIKSHAN PARISHAD'S
ANANTRAO PAWAR COLLEGE OF ENGINEERING & RESEARCH
Sr. No. 103, Parvati, Pune - 411 009.
Tel.: 020-24218901/8959 Tele Fax : 020-24213929
Web.: http://www.abmspcoerpune.org Email : abmspcoe@yahoo.com
Approved by AICTE & Govt. of Maharashtra, Affiliated to Savitribai Phule Pune University
NAAC ACCREDITED, DTE CODE :- EN 6794, AISHE CODE :- C-41484
Savitribai Phule Pune University Identification No. PU/PN/Engg. / 441/2012.

3.3.2: Number of books and chapters in edited volumes/books published per teacher during last five years.

Sr. No.	Name Of Teacher	Title Of Book	Year	ISBN No.	Affiliating Institute	Name Of Publisher	Web Link Of Books
1	Kondhalkar Ganesh Eknath	Artificial Intelligence And Machine Learning	2022	935451534-1	APCOER	Nirali Prakashan, Pune	https://niralibooks.com
2	Ashish Raju Pawar	Computer Aided Engineering	2022	978-93-5585-030-0	APCOER	Technical Publications, Pune	https://technicalpublications.in
3	Deshpande Soojey Ramchandra	Basic Electronics Engineering	2022	2563-5564	APCOER	Nirali Prakashan, Pune	https://niralibooks.com
4	Munde Kashinath Haribhau	Artificial Intelligence And Machine Learning	2022	9789354515347	APCOER	Nirali Prakashan, Pune	https://niralibooks.com
5	Munde Kashinath Haribhau	Solid Mechanics	2022	9789354515293	APCOER	Nirali Prakashan, Pune	https://niralibooks.com

Principal
Anantrao Pawar College of Engineering
& Research, Parvati, Pune - 9

AKHIL BHARATIYA MARATHA SHIKSHAN PARISHAD'S
ANANTRAO PAWAR COLLEGE OF ENGINEERING & RESEARCH
Sr. No. 103, Parvati, Pune - 411 009.
Tel.: 020-24218901/8959 Tele Fax : 020-24213929
Web.: http://www.abmspcoerpune.org Email : abmspcoe@yahoo.com
Approved by AICTE & Govt. of Maharashtra, Affiliated to Savitribai Phule Pune University
NAAC ACCREDITED, DTE CODE :- EN 6794, AISHE CODE :- C-41484
Savitribai Phule Pune University Identification No. PU/PN/Engg. / 441/2012.

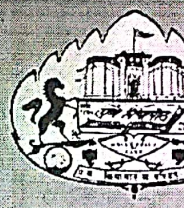
6	Munde Kashinath Haribhau	Computer Aided Manufacturing	2021	9390450853	APCOER	Technical Publications, Pune	https://technicalpublications.in
7	Thakare Sunil Bhimrao	Quantity Surveying,Contracts& Tenders	2021	9789389748413	APCOER	Techknowledge Publications	https://techknowledgebooks.com
8	Gaikwad (Londhe-Patil) Rama B	Object Oriented Software And Web Engineering	2020	B08b1rgckk	APCOER	Nirali Prakashan, Pune	https://niralibooks.com
9	Mahadik Pranali P.	B08b1rgckk	2020	B08b1rgckk	APCOER	Nirali Prakashan, Pune	https://niralibooks.com

Dr.Sunil B. Thakare

Principal

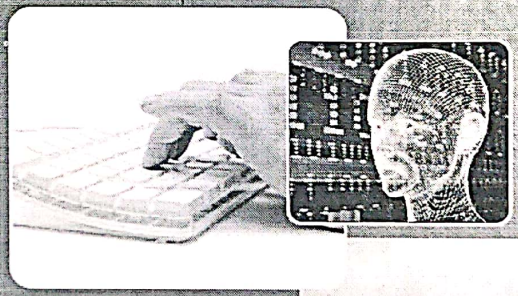
Anantrao Pawar College of Engg & Research * Pune-9 * Pune

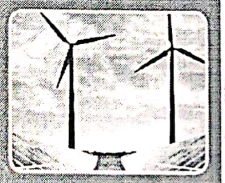
PROCEEDINGS

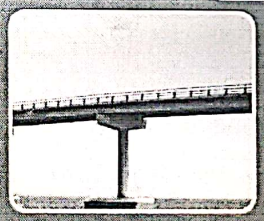


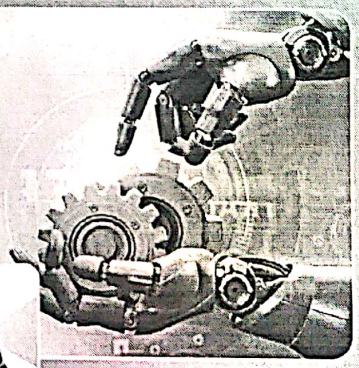
National Conference on Technical Revolution (NCTR- 2018)

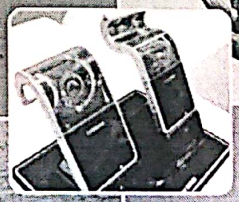
14th - 15th February 2018

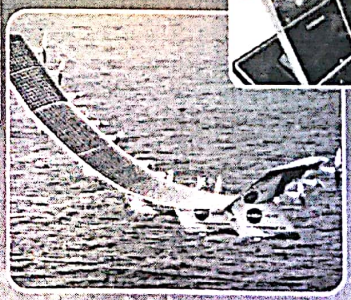












Jointly Organized by

Savitribai Phule Pune University

&

Akhil Bharatiya Maratha Shikshan Parishad 's

Anantrao Pawar College of Engineering & Research, Parvati, Pune-09

ISBN NUMBER
978-81-930856-4-6

INDEX

A Review on Multi Hop Data Aggregation Technique in Mobile Sensing with Security

Tejashree Gaikwad,Department of Computer Engineering ABMSP's APCOERPune, India tejashree.gaikwad@abmspcoerpune.org*

Pranali Mahadik,Department of Computer Engineering ABMSP's APCOERPune, India pranali72@gmail.com

Rama Gaikwad, Department of Computer Engineering ABMSP's APCOER,Pune, India rama.coer@gmail.com

Sneha Ramteke4, Department of Computer EngineeringABMSP's APCOERPune, Indiaramtekemsneha@gmail.com

Abstract: In the coming future of Digital Media Smart Mobile Devices are getting more and more importance. The use of these smart devices in day to today life of human being have been increased and it becomes very easy to share information through these devices to others. These mobile devices are now facilitated with number of applications that are using various sensors like camera, microphone, GPS, accelerometer, ambient light sensor etc. But the data shared by an individual have to be protected. And to maintain the privacy of the important data, the shared data have to be protected. With the help of large numbers of individual participants, aggregation which is computed from data is really useful and helps to predict the statistics of Result. Aggregation guarantees more privacy of the data from individual participants. This paper provides a solution for preserving the individual participants privacy by using aggregate function like Sum, Min. Calculation of Sum aggregation is done without releasing the participant's information. Min aggregation is calculated using Sum aggregation. Min aggregation is nothing but minimum value of data. In this paper, a multi-hop network is considered where, there is a main aggregator at the highest level and mobile nodes are considered at lowest level and in between node sink are used at middle level. This system deals with dynamic leaves and joins in mobile sensing using the timestamp of the participants.

Keywords: Encryption, Multi-hop network, Mobile Sensing, Data Aggregator, Privacy

1.0 INTRODUCTION

The wireless Mobile wireless sensor network can be simply defined as WSN with mobile as sensor nodes. These nodes Consist of a radio Trans receiver and a microcontroller powered by battery. The topology used for this network is not decided. So, routing becomes challenging job. Data Aggregation is nothing but collection of data from different resources or nodes and giving output as a summary. The aggregation statistics are normally computed periodically to analyses its pattern. The data aggregators may generate the source information which are available in public records and databases, this updated information is then transferred into aggregate reports and then may sold to different agencies. These reports can be used in background checks and to make some decisions. Most of the works in this consider that the aggregator is trusted. But this is not the case each time. The challenge is to protect data when the aggregator is untrusted. Many of the recent works[2][3],consider the time series data and untrusted aggregator. In this, for the purpose of protection of data ,a new encryption scheme is introduced. In this schemes ,aggregator decrypts only the sum of all users data instead of individual users data pick before observe the equivalent keyword search trapdoors. It seems an suitable security concept, particularly if the keyword space has no high min-entropy.In this paper, we propose a protocol to get sum aggregate in multi-hop network and considering the untrusted aggregator. In computer networking, a hop

PROCEEDINGS

National Conference on Technical Revolution (NCTR- 2019)

12th - 13th February 2019

Organized by

Akhil Bharatiya Maratha Shikshan Parishad 's

Anantrao Pawar College of Engineering & Research, Parvati, Pune-09

(Accredited By NAAC)

In Association with

Savitribai Phule Pune University, Pune

ISBN NUMBER
978-81-930856-5-3

INDEX

Review on IOT based Natural Disaster Monitoring & Alert System For Earthquake, Fire and Landslides

[1]Amit A. Kadam,[2]J. C. Musale, [3]V. S. Gaikwad, [4]D. S. Lavhkare
[1]Assitant Professor, [2]Associate Professor, [3]Assitant Professor, [4]Assitant Professor
[1]Department of Computer Engineering,
[1]Anantrao Pawar College of Engineering & Research, Pune, India

Abstract: We know that natural disasters like Earthquake, fire and landslides can be proved to be great harm to man-kind. This harm cannot be prevented but by careful planning and emergency steps of spreading alert we can often reduce the consequences of these disasters. Recent technological advances in communication medium made new trend in monitoring system. These new systems focuses on monitoring water level earth vibration room temperature via sensors, and generate alert signals when the values cross the threshold values provided to sensors. Alert message is a Text Message and Android application notification services to the concerned authorities through their mobile phones. It also includes public address (PA) system to broadcast the message to local peoples nearby the place. The module can also send the water level to the android user. This app will be very useful to the community and can used as a primary precaution action to save many lives.

Index Terms **– Earthquake, fire, landslides, IoT, Disaster Management.**

I. INTRODUCTION

Natural calamities such as earthquakes, fires, and landslides pose significant challenges to humanity. While these disasters are unavoidable, the impact can often be mitigated through meticulous planning of emergency responses, including 'alert' systems. Advances in communication technology have paved the way for innovative trends in disaster monitoring systems. These systems are designed to track water levels, room temperatures, and seismic activities using sensors. They trigger an alert when measurements exceed preset thresholds. Alerts are delivered as text messages and notifications through an Android application to relevant authorities' mobile devices. Additionally, the system is equipped with a Public Address (PA) system for broadcasting messages to locals, especially those near forested areas. The module is also capable of transmitting water level updates to users of the Android App.

A natural disaster refers to a significant adverse event caused by the natural workings of the Earth, such as floods, hurricanes, tornadoes, volcanic eruptions, earthquakes, tsunamis, and other geological phenomena. Natural disasters can lead to loss of life, damage to property, and typically result in some degree of financial loss, the extent of which varies based on the resilience of the affected population and the available infrastructure.

An event does not reach the magnitude of a disaster if it occurs in an area without a vulnerable population. However, in regions with susceptible communities, such as Nepal during the 2015 earthquake, an earthquake can result in devastating impacts and long-term damage, necessitating extensive recovery efforts.

1.1 Scope

Scope of our system defined as that can be used in real time purposed. It's more usable to disaster management like departments who keeps monitoring on natural disaster. This system can be very use in keeping track of all the disastrous activities and will help as taking primary step in saving people's lives.

1.2 Compensating for limited Infrastructure

IoT technologies offer significant potential in enhancing disaster preparedness and response, particularly through forecasting and early warning systems. These technologies can be especially beneficial in developing and emerging countries, where infrastructure limitations make these areas more susceptible to the impacts of disasters. For instance, in the context of forest fire monitoring, sensors placed on trees can measure various indicators such as temperature, humidity, and carbon dioxide levels to detect the onset of a fire or assess the risk of one occurring. When these sensors detect a hazardous combination of these parameters, early warning systems can then alert local populations and signal for assistance. Upon their arrival, firefighters are equipped with precise information regarding the fire's location and extent, enabling more effective response efforts.

Furthermore, the development of IoT applications spans various types of disasters. This includes the use of microwave sensors to monitor earth movements that could indicate an impending earthquake, as well as infrared sensors designed to identify and assess flood risks and human movement patterns. These innovations underscore the role of IoT in improving disaster watchfulness and mitigating the consequences of natural catastrophes.

II. WORK

The integration of advanced technologies like IoT, cloud computing, and fog computing into disaster management systems presents a promising avenue for enhancing disaster preparedness and response efforts. Here's a summary of the key points from the papers discussed:

Study on Cyber Security applicable for digitallife

[1] Pranali Prakash Mahadik, [2] Rama Gaikwad

[1,2] Assistant Professorr,

[1,2] Department of Computer Engineering,

[1,2] Anantrao Pawar College of Engineering & Research, Pune, Maharashtra, India

Abstract: There is considerable overlap between cyber security and information security but these both concepts are totally different. Cyber security is goes beyond information security it include only protection for information resources. In information security reference to the human factor usually relates to the role of human in security process but in cyber security human is target of cyber-attack. Main aim of Cyber Security is of protecting information and various information systems such as database, networks, different data centers and various applications by using suitable procedural and technological security measures.

Now a days to protect personal data only firewall, antivirus software are not sufficient. Because now a day's cyber infrastructure is speedily growing and Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be included in the educational. Security counter measure helps ensure the confidentiality, availability and integrity of information systems by preventing or serious asset losses from Cyber Security attacks.

IndexTerms **- Cyber Security, Threats, Cyber safety, Cyber attack**

I. INTRODUCTION

Cyber security is crucial for protecting cyberspace from various cyber-threats, encompassing both malicious acts targeting or using communication technology. It plays a vital role in developing information technology and internet services, ensuring the protection of software, hardware, and personal information. Cyber security efforts must cover several elements, including application, operational, network, end-user education, information security, and disaster recovery.

1.1 Information security

Information security is also called as InfoSec, main aim is to prevent unauthorized access, modification, use, inspection, disclosure, recording, destruction and disruption of information. The information also refer to data in any form like physical or electronic. InfoSec's mainly focus on integrity, confidentiality and availability of data.

It is significant to note that there is a difference between information and communication technology security and information security

1.2 Information and communication technology security

Information and communication technology (ICT) security related with the providing protection to the technology-based systems on which information is commonly stored and transmitted. And information security include the protection to the fundamental information resources.

ICT have additional characteristics like include non-repudiation, accountability, authenticity and reliability.

II. THREATS TO CYBER SECURITY

Information security (InfoSec) is dedicated to preventing unauthorized access, alteration, or disruption of data, in any form. It prioritizes data integrity, confidentiality, and availability. InfoSec differs from Information and Communication Technology (ICT) security, which focuses on protecting the tech systems used for information storage and transmission, incorporating principles like non-repudiation, accountability, authenticity, and reliability.

Cyber security threats are dynamic and innovative, constantly finding new methods to damage or exploit cyber systems either for destructive purposes or for illicit gains without necessarily compromising the infrastructure. These threats can subtly infiltrate systems, allowing for actions that can gradually degrade a system's functionality.

2.1 Examples of Online Cyber security Threats

2.1.1Computer Viruses

Computer virus is most renowned threat for computer security It is a program written to modify the way by which a computer operates, without the authorization or knowledge of the user. Computer virus replicates and executes itself typically doing damage to computer.

To avoid Computer virus avoid downloading from peer-to-peer file sharing site ,evaluate free software's and emails.

Comparison over Encrypted Data for Privacy Preservation Based on Homomorphic Encryption

[1] Vijayendra S. Gaikwad, [2]Amit A. Kadam, [3]Jitendra C. Musale, [4]Rahul B. Diwate
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor
Department of Computer Engineering,
APCOER, Pune, India

Abstract: Now a days, with data mining computation being performed by cloud servers it is a problem to securely determining whether x>y, given two input values x, y, which are held as private inputs by two parties, respectively. The output which is result of comparison becomes known to both parties. In this paper we consider a variant of comparison problem in which the inputs x, y are encrypted and the actual values are not known to the parties. Our solution deals with single comparison; however, in many applications, we encounter situations where it is necessary to make multiple comparisons to find the maximum among several encrypted data, so we make a modification to our protocol to solve the multiple comparisons problem. Such a secure comparison is an important building block for applications like privacy preserving data mining and secure business. Also our protocols can be performed in constant rounds and do not use general circuit evaluation techniques so they are more efficient than circuit based ones but not general. Implementation is easy and fast.

***Index Terms*–Secure two party computation; multiple comparisons, Encrypted data**

I. INTRODUCTION

About two decades ago, Yao introduced the "millionaire problem" [1]: Two parties want to determine who is richer without disclosing anything else about their wealth. Several solutions have been proposed for this problem; however, none of them consider our issue. In addition there are some limitations with Yao's Millionaire Problem; we call this problem YMP in short in this paper.

YMP is applicable with just one comparison, i.e. a comparison between two numbers. However, we may face lots of situations where there are several numbers (e.g n numbers) to be compared. This problem cannot be solved by just using the basic Yao's Millionaire solution n-1 times, once for each pairs. For two reasons this approach is not suggested. Applying Yao's solution several times not only reduces the performance but also effects on privacy, because that would inappropriately reveal the relative ordering between pairs which causes information leakage.

Another limitation; YMP does not considered situation where encrypted data should be compared and actual values are not known to parties.

To explain the issue which is addressed in this paper, consider the following scenario:

Alice and Bob owning private databases wish to run a decision tree algorithm on the union of their databases. Since the databases are confidential, neither of them is willing to disclose any of the contents to the other. Lindell and Pinkas have shown that how to construct decision tree by cooperation without disclosing of private data in [10]. As we know the important step to build a decision tree is choosing best attribute for branching, for example in ID3 algorithm the best attribute is chosen based on Information gain. After two parties compute information gain for each attribute in privacy preserving manner, it is time to determine the maximum information gain.

Alice acts as server and works over his data and Bob's encrypted data and computes information gain in encrypted form while Bob owns the decryption key. Due to privacy considerations Alice would not send all encrypted values to Bob. So they should run a protocol to find the attribute with maximum information gain.

Another requirement is that the actual values of Information gain should not be clear to any parties and should not going to be revealed at the end of protocol, only the result (selected attribute) is important for decision.

We call this problem, "comparison over encrypted data" in this paper. "Comparison over encrypted data" can be extended into three issues that we propose solutions for each one.

Alice and Bob want to compute a function on their private inputs; the initial output is two cipher texts (C1 and C2). The problem is to securely determine whether actual value of C1 or C2 is greater. Our solution to this problem is general.

According to mentioned scenario; sometimes we have more than two numbers (n) to be compared. The requirement of not allowing each party to know any partial information about the individual comparisons immediately rules out using our first solution n-1 times. A new protocol is proposed to solve such "comparison *over encrypted data*" problem by extending the first solution.

"Comparison over encrypted data" is an important building block for applications such as privacy preserving data mining and secures business. For example two companies (A, B) determine to aware of the product with highest sale. A has an n-dimensional vector A= (a_1, a_n) and B has another n-dimensional vector B= (b_1, b_n). a_i and b_i show the number of sales for a specific product. B encrypts its elements and sends to A then A adds his values to received values via Homomorphic encryption. After that