Sum Aggregation of Time – Series Data with new Preserving System

T.Manasa
Computer Science and Engineering
MITS College, Madanapalle, Andhra Pradesh, India

Abstract:- *The usages of mobile devices are increasing rapidly. Such as a smart mobiles and having the variety of mobile sensing applications. Here we may note that the most previous works on the sensor data aggregation assume a trusted aggregator and in mobile sensing applications cannot facilitating the protect user privacy against an un trusted aggregator. Here they do not consider the data aggregation. To attain that we derived a new privacy-preserving protocol. To perform efficient aggregation the techniques like Homomorphism encryption and a novel, HMAC based key management are utilized. We projected two method to derivating the Min aggregation of the time series data. In that first can attain accurate Min, another one attain approximate Min. With this attestable blunder certification at a great deal of low cost. For managing the dynamic joins and leaves we are proposed a scheme. That can exploit the redundancy in security to decreasing the communication cost for every join and leaves. The simulation results can show how much our scheme has much lower communication overhead then exist.*

1. INTRODUCTION

Without compromising the privacy of each user in mobile sensing we mainly focus on how an un trusted aggregator in mobile sensing can periodically attain desired statistics with the data provided by many mobile users, Decreasing the communication cost. Sometimes it may lead to crash data, So as to we are implementing the Additive Encryption and Multiplicative Encryption.

It also attain the more security. To perform efficient aggregation the techniques like Homomorphism encryption and a novel, MAC based key management are used in this we providing effective privacy to the data.

Our main objective is to propose a new protocol for mobile sensing to obtain the sum aggregate of time-series data in the presence of an untrusted aggregator. The protocol utilizes additive homomorphic encryption and a based key management technique to perform extremely efficient aggregation. It deals with dynamic user joins and leaves.

Secure Computing consisted of several merged units, one of the oldest being Enigma Logic, Inc., which was started around 1982. Bob Bosen, the founder, claims to have created the first security token to provide challenge-response authentication. Secure Computing acquired the SmartFilter product line by purchasing Webster Network Strategies, the producer of the WebTrack product, in 1996.The acquisition included the domain name webster.com, which was eventually sold to the publishers of Webster's Dictionary.

Cloud computing is alike grid computing. It was invented in 1994 by AT&T(Andy Hertfeld & BillAtrinson) two of original engineers on the Apple Macintosh. Cloud computing is a recently evolved computing terminology based on utility and consumption of computing resources. Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid.

Motivation

An important goal of this work to providing security to users data while transferring from one place to another. While transferring data, an untrusted aggregator may leads to loss the users data. Most previous works on sensor data aggregation assume a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. So,we are implementing the encryption algorithms for providing security to the data and also reducing the communication cost for each join and leave.

In this project, we proposed a new protocol for mobile sensing to obtain the sum aggregate of time series data in the presence of untrusted aggregator. Based on the sum aggregate protocol, we

propose a protocol to obtain the Min aggregate. Its also supporting large plain text spaces. It requires only a single round of user-to-aggregator communication.

2.Requirement Analysis

In software engineering (and systems engineering), a functional requirement defines a function of a system and its components. A function is described as a set of inputs, the behavior, and outputs (see also software).

Functional requirements may be calculations, technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish. Behavioral requirements describing all the cases where the system uses the functional requirements are captured in use cases. Functional requirements are supported by non-functional requirements (also known as quality requirements), which impose constraints on the design or implementation (such as performance requirements, security, or reliability). Generally, functional requirements are expressed in the form "system must do <requirement>", while non-functional requirements are "system shall be <requirement>". The plan for implementing functional requirements is detailed in the system design. The plan for implementing non-functional requirements is detailed in the system architecture.

Existing System

Many works have addressed various security and privacy issues in mobile sensing networks and but they do not consider data aggregation. There are a lot of existing works on security and privacy-preserving data aggregation, but most of them assume a trusted aggregator and cannot protect user privacy against untrusted aggregators. The current encryption scheme allows an untrusted aggregator to obtain the sum of multiple user's data without knowing any specific user's data. However, this scheme requires expensive rekeying operations to support multiple time steps, and thus may not work for time-series data. The privacy-preserving data aggregation scheme based on data slicing and mixing techniques is not designed for time-series data. It may not work well for time-series data, since each user may need to select a new set of peers in each aggregation interval due to mobility. Besides, the scheme for nonadditive aggregates (e.g., Max/Min) requires multiple rounds of bidirectional communications between the aggregator and mobile users which means long delays.

Disadvantages of Existing System

- Min aggregate which is quite useful in mobile sensing which are not considered by the existing systems.
- High Computation is required which leads delay.
- Most Existing systems works on sensor data aggregation.
- User privacy cannot be protected against an untrusted aggregator in mobile sensing applications.

In order to make the data secure we are using two new encryption techniques named

1) Additive encryption

2) Multiplicative encryption

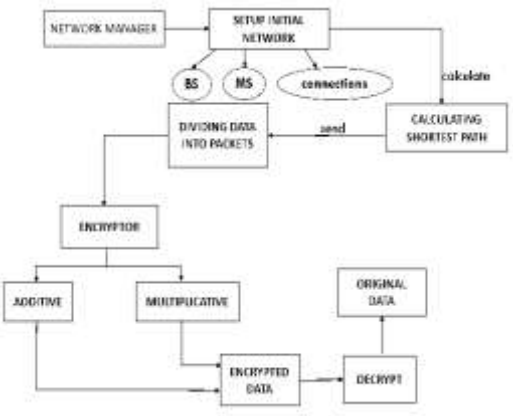

Fig.1: Technical Architecture

Additive Encryption

This is a type of encryption which uses a single encryption algorithm with 2 different keys and apply it to the data packets alternately so that the security of the data is maintained. In this project the algorithm that is used in this encryption is AES.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES), also referenced as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process.Rijndael is a family of ciphers with different key and block sizes.For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001.This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable (see Advanced Encryption Standard process for more details).

AES became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.The name Rijndael is a play on the names of the two inventors (Joan Daemen and Vincent Rijmen). It is also a combination of the Dutch name for the Rhine river and a Dale.

Multiplicative encryption

This is a type of encryption which uses two algorithms for encryption Here we are using AES and MD-5, the secret key foe AES algorithm will be generated automatically and the secret key for MD-5 is be manual.

MD-5

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verifydata integrity.MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function, MD4.The source code in RFC 1321 contains a "by attribution" RSA license.

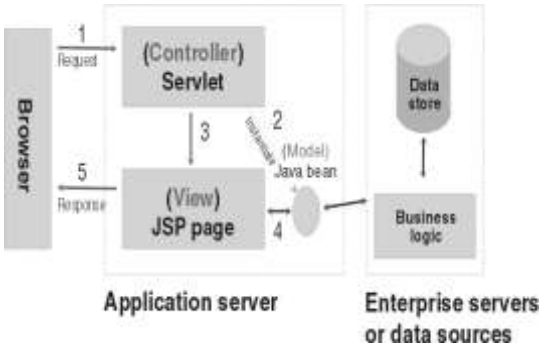

Fig.2: System Architecture

1. The browser sends a request to a servlet.

2. The servlet instantiates a Java bean that is connected to a database.
3. The servlet communicates with a JSP page.
4. The JSP page communicates with the Java bean.
5. The JSP page responds to the browser.

Proposed System

We are going to develop a proposed system to facilitate the collection of useful aggregate statistics in mobile sensing without leaking mobile users' privacy, we proposed a new privacy-preserving protocol to obtain the Sum aggregate of time-series data. The protocol utilizes additive homomorphic encryption and a novel, HMAC based key management technique to perform extremely efficient aggregation. Implementation-based measurements show that operations at user and aggregator in our protocol are orders of magnitude faster than existing work. Thus, our protocol can be applied to a wide range of mobile sensing systems with various scales, plaintext spaces, aggregation loads, and resource constraints. Based on the Sum aggregation protocol, we also proposed two schemes to derive the Min aggregate of time-series data. One scheme can obtain the accurate Min, while the other one can obtain an approximate Min with provable error guarantee at much lower cost. To deal with dynamic joins and leaves, we proposed a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave. Simulation results show that our scheme has much lower communication overhead than exist.To facilitate the collection of useful aggregate statistics in mobile sensing without leaking mobile users' privacy, we proposed a new privacy-preserving protocol to obtain the Sum aggregate of time-series data.

Advantages of Proposed System

- Providing large plain text space.
- More security to the data and also reducing the crashes.
- As long as privacy to the data sharing.
- Finds shortest path to the data packets
- Reducing the communication cost of dealing with dynamic joins and leaves.

Key features:

Dealing with dynamic joins and leaves

It deals with dynamic joins and leaves. When this application is used in mobile networks, we have an advantage that the secret key which is given to one user is not revealed to the other one which means that the data will not be reveals to the next node user or previous user. The new user who joins the network cannot receive the data which is going to be communicated next and the old user who has left the network cannot receive the current information.

Affiliation

The affiliation of a secret is the user that it is assigned to.Every user will be given a secret key in order to receive or transmit the data in this process of data transfer the secret key which is given to the user in order to decrypt the data is termed as affiliation.

Forward Security

This is one feature of affiliation. After the join (leave) operation, the key that an entity will use in the future is secure, i.e., the probability that the adversary can successfully guess the key in a single trial is not higher than 2^{-}. The main intention of this is that once a user has left the network , to make the future data that is going to be transmitted secure we are providing a particular size of the key.

Backward Security

This is the second main feature of affiliation After the join (leave) operation, the key that an entity used in the past is still secure, i.e., the probability that the adversary can successfully guess the key in a single trial is not higher than $2^{-l..}$. These features play a major role in the efficiency of the entire project.

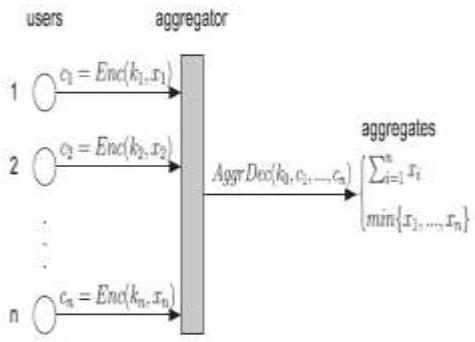

Fig 3: Encryption Techique

3.Modules

There are six modules. They are as follows:

1) Network setup

2) Calculating multiple shortest paths

3) Data packetization

4) Additive encryption

5) Multiplicative encryption

6) Decryption

Network setup

In this module administrator of network can create a network completely by including number of nodes, connects between nodes, paths and bandwidth etc. This is nothing but making initial network setup.

Calculating shortest paths

In this module we are going to develop logic for identifying n shortest paths between source and destination. Instead of sending data from single shortest path if we send data from multiple shortest paths then data will be delivered with speed.

Data packetization

In this module we are going to develop logic for dividing data into different sizes of packets basing data carrying node. By partitioning data into suitable sizes of packets then there is no drops can happen while transferring data.

Additive encryption

This is one of the encryption techniques where data can be divided into two different parts where each part can be encrypted with different keys for encryption algorithm.

Multiplicative encryption

In this data can be divided in two parts and each part can be encrypted with different algorithms and then that two encrypted data can be concatenated.

4.Tables

Validation for login Page

S.no	Field Name	Validations	Messages	Remarks
1)	Email	Format is example@pattern.com Email should not be empty	Email is Required	Cannot be navigated
2)	Pass word	Password Should not be empty	Password is Required	Cannot be navigated

Table 1: Login Validate Page

It shows that how to enter the main page. It validates the user containing mail ID and password are correct or not. If the Email and password are correct,then it enters the home page.Otherwise, cannot be navigated and it displays email and password are not correct.

Test case for login page

S.no	Check Item	Test case Objective	Test Data / Input	Expected Result	Actual Result	Results
1	Log-in Page	Leave all fields as blank and click Log-in button		By leaving all fields as blank and on click Log-in button then we get e mail id is wrong	By leaving all fields as blank and on click Log-in button then we get email id is wrong	PASS
2	User name	Enter Invalid Username	Username : 94925226ab	By entering invalid Username then an error message should appear as " login id is wrong "	By entering invalid Username then an error message appeared as" login id is wrong "	PASS
3	User name	Enter valid Username	Username : 9492522678	It should allow the user to proceed	allowed user to proceed	PASS
4	Password			The password field should display the encrypted format of the text typed as ****	Password field displayed in encrypted format of the text typed as ****	PASS
5	Password	Enter wrong password	Password : ***	By entering invalid password then an error message should appear as " Please Enter Correct Password "		
6	Password	Enter Correct password	Password : ********	It should allow the user to proceed	allowed user to proceed	PASS
7	Log-in button	Correct Inputs		It should lead the user to the respect page	allowed user to respective page	PASS

Table 2: Login Test Case

Table structure for table msgdata

This table is for table msg data. It contains seven fields such as

1) msgid
2) msgdata
3) suserid
4) duserid
5) algid
6) kid
7) spid

Column	Type	Null	Default
Msgid	int(11)	No	
msgdata	Longtext	No	
suserid	int(11)	No	
duserid	int(11)	No	
Algid	int(11)	No	
Kid	int(11)	No	
Spid	int(11)	No	

Table 3: Structure of Meassage Data

It represents to send data from souce to destination. It shows to create the data table and it contains some properties for sending data more securily.

5.Conclusion

The protocol utilizes additive encryption and a multiplicative encryption to perform extremely privacy. Implementation-based measurements show that operations at user in our protocol are orders of magnitude faster than existing work. Results show that our scheme has much lower communication overhead than existing work.

6.Future Enhancement

- The research is going on to still improve the Security and make the data transfer more secure.
- In future, this protocol may extend to various platforms and increase its efficiency in retrieving the time series data.

7.Reference

[1] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M.Hansen, E. Howard, R. West, and P. Boda, "Peir, the PersonalEnvironmental Impact Report, As a Platform for ParticipatorySensing Systems Research," Proc. ACM/USENIX Int'l Conf. MobileSystems, Applications, and Services (MobiSys '09), pp. 55-68, 2009
[2] " Security and High availability in cloud computing environments" , IBM Global Technology Services June 2011
[3] "Swamp Computing" a.k.a cloud computing
Web security Journal. 2009-12-28.
[4] V. Krishna Reddy, B. thirumal Rao, Dr. L.S.S Reddy, P.Sai Kiran "Research Issues in Cloud Computing" Global Journal of Computer Science and Technology volume 11, Issue 11, July 2011.
[5] "Thunder Clouds: Managing SOA-Cloud Risk",Philip Wik". Service Technology Magazine.2011-10-21.
[6] Nidhi Singhal, J.P.S. Raina – Analysis of AES Algorithm for Better Utilization.
[7] Sherin, Sreedharan, G.Kalpana- Security Issues and solutions for Cloud Computing.
[8] Jackson Higgins, Kelly (May 19, 2008). "Permanent Denial-of-Service Attack Sabotages Hardware". Dark Reading. Archived from the original on December 8, 2008.
[9] Ms.S.Kavitha , Ms.P.Aruna Devi , Ms.P.Sudha – Mobile Computing Denial of Service
[10] V. Rastogi and S. Nath, "Differentially Private Aggregation ofDistributed Time-Series with Transformation and Encryption,"Proc. ACM SIGMOD Int'l Conf. Management of Data, 2010.