ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 22-27 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp05.pdf

FRAMEWORK FOR SECURE AND EFFICIENT DATA AGGREGATION IN NETWORK SENSING

Mr. B.Narendra[1], Mr.AVSSudhakar Rao[2]

[1]*II M.Tech. - II Sem., Dept. of CSE, St. Ann's College of Engineering. & Technology. Chirala, Andhra Pradesh -,523 187 INDIA,*
507narendra @gmail.com

[2] *Associate Professor Dept. of CSE, St. Ann's College of Engg. & Tech., Chirala, A. P, INDIA*
ande_sudhakar@yahoo.co.in

ABSTRACT:-

The multiplication and continually expanding capacities of cell phones, for example, advanced mobile phones offer ascent to a mixed bag of portable detecting applications. This paper thinks about how an untrusted aggregation in portable detecting can occasionally acquire wanted insights over the information contributed by various versatile clients, without bargaining the security of every client. Albeit there are some current works here, they either require bidirectional correspondences between the aggregation and portable clients in every conglomeration period, or have high calculation overhead and can't bolster huge plain text spaces. Likewise, they don't consider the Min total which is very valuable in portable detecting. To address these issues, we propose a productive convention to acquire the Sum total, which utilizes an added substance homomorphic encryption and a novel key administration procedure to bolster substantial plain text space. We likewise extend the entirety conglomeration convention to get the Min total of time arrangement information. Assessments demonstrate that our conventions are requests of size quicker than existing arrangements.

INTRODUCTION:-Cell phones, for example, advanced mobile phones are picking up a continually expanding prevalence. Most advanced cells are furnished with a rich arrangement of installed sensors, for example, camera, amplifier, GPS, accelerometer, surrounding light sensor, gyrator, and so on. [1] The information produced by these sensors gives chances to make refined inductions about not just individuals (e.g., human action, wellbeing, area, get-together) additionally their encompassing (e.g., contamination, clamour, climate, oxygen level), and subsequently can help enhance individuals' wellbeing and in addition life. This empowers different portable detecting applications, for example, natural observing, movement checking, social insurance, and so on. In numerous situations, collection measurements should be intermittently registered from a flood of information contributed by portable clients, so as to recognize some phenomena or track some vital examples. Case in point, the normal measures of every day exercise (which can be measured by movement sensors) that individuals do can be utilized to gather general wellbeing conditions. The normal or greatest level of air contamination and dust fixation in a range may be helpful for individuals to arrange their outside exercises. Different insights of intrigues incorporate

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 22-27 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp05.pdf

the most reduced fuel cost in a city, the most elevated moving rate of street activity amid surge hour, and so on. Despite the fact that accumulation measurements processed from time-arrangement information is extremely valuable, in numerous situations, the information from individual client may be protection touchy, [2] and clients don't believe any single outsider aggregator to see their information in clear content. Case in point, to screen the engendering of influenza, the aggregator will check the quantity of clients contaminated by this influenza. On the other hand, a client may not have any desire to straightforwardly give her actual status ("1" if being tainted and "0" generally) in the event that she is not certain whether the data will be mishandled by the aggregator. In like manner, frameworks that gather clients' actual information values and process total insights over them may not meet clients' protection prerequisite. In this manner, an essential test is the way to ensure the clients' security in portable detecting, particularly when the aggregator is untrusted.[2], [3]

Most past deals with sensor information accumulation expect a trusted aggregator, and henceforth can't secure client protection against an untrusted aggregator in versatile detecting applications. A few late worksconsider the collection of time arrangement information in the vicinity of an untrusted aggregator. To ensure client protection, they outline encryption conspires in which the aggregator can just unscramble the total of all clients' information however nothing else. Rastogi and Nath use edge Paillier cryptosystem to fabricate such an encryption plan. To decode the whole, their plan needs an additional round of cooperation between the aggregator and all clients in every total period, which implies high correspondence cost and long defer. In addition, it obliges all clients to be online until decoding is finished, which may not be down to earth in numerous versatile detecting situations because of client portability and the heterogeneity of client integration. Riffle et al.[4] propose a development that does not require bidirectional interchanges between the aggregator and the clients; however it has high reckoning and stockpiling expense to manage conspiracies in an expansive system.

RELATED WORK:-

Numerous works have tended to different security and protection issues in versatile detecting systems and frameworks (e.g.,), yet they don't consider information total. There are a ton of existing works (e.g.,) on security and protection saving information total, yet a large portion of them expect a trusted aggregator and can't ensure client protection against untrusted aggregators. Yang et al. proposed an encryption plot that permits an untrusted aggregator to acquire the total of different clients' information without knowing any particular client's information. On the other hand, their plan requires lavish re-keying operations to bolster various time steps, and accordingly may not work for time-arrangement information. Shi et al. proposed a protection saving information accumulation plan taking into account information cutting and blending strategies. Notwithstanding, their plan depends on distributed interchanges among clients, which is nontrivial in versatile detecting situations because of the high portability of clients. Additionally, their plan does not function admirably for time-arrangement information, since every client may need to choose another arrangement of companions in every collection interim because of versatility.[7] Moreover, their plan for non-added substance totals

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 22-27 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp05.pdf

(e.g., Max/Min) obliges numerous rounds of bi-directional correspondences between the aggregator and portable clients which means long postpones. Interestingly, our plan acquires those totals with only one round of unidirectional correspondence from clients to the aggregator. To accomplish protection saving entirety collection of time arrangement information, Rastogi and Nath outlined an encryption plan in light of edge Paillier cryptosystem, where the decoding key is partitioned into segments and appropriated to the clients. The aggregator gathers the figure writings of clients reproduces them together and sends the total figure content to all clients. Every client decodes an offer of the total. The aggregator gathers every one of the shares and gets the last total. On the other hand, their plan requires an additional round of connection between the aggregator and clients in every collection period. Taking into account an effective added substance homomorphic encryption plan, Rieffel et al. proposed a development that does not require an additional round of communication between the aggregator and the clients. In their plan, the processing and stockpiling expense is generally equivalent to the quantity of plotting clients that the framework can endure. Accordingly, their plan has high overhead to accomplish great imperviousness to arrangement, particularly when the framework is huge and countless connive. Interestingly, our plan endures a high portion of conniving clients (e.g., 30%) with little cost notwithstanding when the framework is substantial. Acs and Castelluccia additionally proposed a plan in light of added substance homomorphic encryption, yet in their plan every hub imparts a pairwise key to some other node.

ALGORITHMS:-

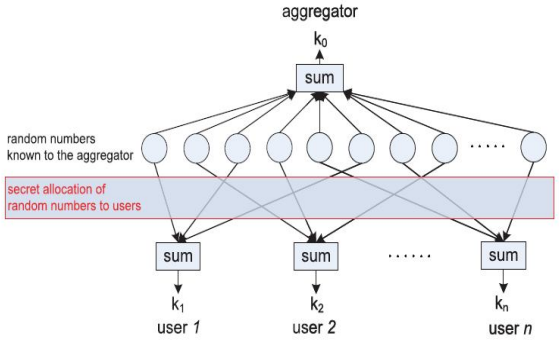
❖ The data perturbation algorithms proposed in and then the sum of noisy data is obtained using our protocol.

❖ Relaxing the assumption of trusted key dealer: Instead of relying on a trusted key dealer, our protocol can be easily adapted to work with an honest-but-curious key dealer that does not collude with the aggregator.

❖ More aggregate statistics: In the basic aggregation scheme for Min presented. The aggregator can actually get the number of times that each possible data value appears and derive the accurate distribution of the user's data in the plaintext space.

❖ Fault tolerance: Fault tolerance requires that when a number of users fail (e.g., due to loss of power or network connection), the aggregator can still get the aggregate statistics of the remaining users.

❖ Weaker assumption on colluders. In previous sections, we assumed that is the maximum accumulated fraction of colluding users in the lifetime of the system.



This paper studies how an un trusted aggregator in mobile sensing can periodically obtain desired statistics over the data contributed by multiple mobile

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 22-27 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp05.pdf

users, without compromising the privacy of each user.This enables various mobile sensing applications such as environmental monitoring, traffic monitoring, healthcare, and so on.Since such communication is nontrivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons.Note that this paper focuses on thwarting attacks against users' privacy.Our goal is to guarantee the privacy of each user's data against the untrusted aggregator.Dynamic joins and leaves should be properly dealt with to protect each user's privacy and ensure the secrecy of the aggregate statistics.Differential privacy for Sum. Differential privacy provides strong privacy guarantee for users such that a user's participation in the system only leaks negligible information about the user.The data generated by these sensors provide opportunities to make sophisticated inferences about not only people but also their surrounding and thus can help improve people's health as well as life.In each time period, a mobile user sends her encrypted data to the aggregator via Wi-Fi, 3G or other available access networks.The remainder of this paper is organized as follows: Section 2 discusses related work. Section 3 presents system models and assumptions.An aggregator wishes to get the aggregate statistics of n mobile users periodically.

Shi et al. proposed a development for entirety total in light of the suspicion that the Decisional Diffie-Hellman issue is hard over limited cyclic gatherings. In their development, every client sends her figure content to the aggregator and no correspondence is required from the aggregator to the clients. To decode the total, their development needs to navigate the conceivable plaintext space of whole, and along these lines it is not proficient for a substantial framework with vast plaintext spaces. Chan et al. developed the development in with a paired interim tree system, yet their plan still has the confinement in plaintext spaces. Jawurek and Kerschbaumproposed a plan which gives differential protection to aggregate. Our total convention for aggregate can be utilized as a building square of their plan to enhance the computational proficiency. Additionally, existing works don't consider the Min of time-arrangement information.

a) Models and Assumptions: -Figure 1 shows our system model, which is similar to the model in. An aggregator wishes to get the aggregate statistics of n mobile users periodically, e.g., in every hour. The time periods are numbered as 1, 2, 3.., etc. In every time period, each user i encrypt her data xi with key ki and sends the derived ciphertext to the aggregator. From the ciphertexts, the aggregator decrypts the needed aggregate statistics using her aggregator capability k0. The value of each user's data is an integer within range [0, Δ]. Two types of aggregate statistics are considered in this work, [8] which are Sum and Min. Sum is defined as the sum of all users' data and Min is defined as the minimum value of the users' data. From Sum and Min,many other aggregate statistics can be easily derived, such as Count (i.e., the number of users that satisfy certain predicate), Average (which is derivable from Sum and Count), and Max (which can be obtained from the Min of $\Delta - x$).

In each time period, a mobile user sends her encrypted data to the aggregator via Wi-Fi, 3G or other available access networks. No peer-to-peer communication is required among mobile users, since such communication is nontrivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons. [9]We consider an untrusted aggregator that is

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.3. No.10, Pages : 22-27 (2015)
Special Issue of ICACSSE 2015 - Held on October 30, 2015 in St. Ann's College of Engineering & Technology, Chirala, AP, India
http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp05.pdf

curious about each individual user's data. The aggregator may eavesdrop all the messages sent from/to every user. A number of users may collude with the aggregator, and reveal their data to the aggregator. A number of users may also collude to obtain the aggregate. Similar to, we assume that the fraction of users that collude with/against the aggregator is at most γ ($0 \leq \gamma < 1$), and the system has a priori estimate over the upper bound of γ which can be used in practice. In addition, the aggregator and users have limited computation capability. We assume a trusted authority which issues proper keys to the users and the aggregator via a secure channel. Our goal is to guarantee the privacy of each user's data against the untrusted aggregator, i.e., the aggregator obtains the aggregate statistics without knowing any individual user's data. [10] Note that we aim to protect the privacy of data content not data source. Also, we aim to guarantee that any party without an appropriate aggregator capability obtains nothing. Malicious users may also perform data pollution attacks in which they provide false data values in order to sway the final aggregate statistics. Data pollution attacks are outside the scope of this paper, and their influence can be bounded if each user uses a non-interactive zero-knowledge proof to prove that her data lies in a valid range.

b) Underlying Encryption Scheme:-

One building block of our solution is the additive homomorphic encryption scheme proposed by Castelluccia et al. This scheme works as follows. Encryption:

1) Represent message m as integer $m \in [0, M - 1]$ where M is a large integer.

2) Let k be a randomly generated key, $k \in \{0, 1\}\lambda$, where λ is a security parameter.

3) Output ciphertext $c = (m + h(fk(r))) \bmod M$, where fk is a pseudorandom function (PRF) that uses k asa parameter, h is a length-matching hash function (see details below) and r is a nonce for this message.

Output plaintext $m = (c - h(fk(r))) \bmod M$.

The PRF fk is a function of the PRF family $F\lambda = \{fk: \{0, 1\}\lambda \rightarrow \{0, 1\}\lambda\}k \in \{0,1\}\lambda$ indexed by k. Since provably secure PRFs are usually computationally expensive, Castelluccia et al. advocate using keyed hash functions (e.g., HMAC) as PRFs. HMAC is a PRF if the underlying compression function of the hash function in use is a PRF. When HMAC is used, fk(r) is the HMAC of r with k as the key. The purpose of h is to shorten a long bit string. It maps the output of fk to a shorter bit string of length α, where α is the modulus size of M (i.e., $\alpha = |M|$). H is not required to be collision-consistent, but its output should be uniformly distributed over $\{0, 1\}\alpha$. An example construction for h is to truncate the output of fk into shorter bit strings of length α, take exclusive-OR on all these strings and use it as the output of h. This scheme is proved to be semantically secure. This scheme allows additive homomorphic encryption. Given two ciphertexts $c_1 = (m_1 + h(fk(r))) \bmod M$ and $c_2 = (m_2 + h(fk(r))) \bmod M$, an individual that knows k and k can compute the sum of m1 and m2 directly from the aggregate ciphertext $c = c_1 + c_2$:

$$m = m_1 + m_2 = (c - h(fk(r)) - h(fk(r))) \bmod M. T$$

To correctly compute the sum of n messages $m_1, m_2, ..., m_n$, M must be larger than $n\ i=1\ mi$. In practice, M should be selected as $M = 2^{[\log_2 (\max_i (m).n)]}$

CONCLUSION:-

To encourage the gathering of helpful total insights in portable detecting without releasing

versatile clients' protection, we proposed another security saving convention to get the Sum total of time-arrangement information. The convention uses added substance homomorphic encryption and a novel, HMAC-based key administration strategy to perform to a great degree proficient accumulation. Correlations in view of seat stamping estimation information demonstrate that operations at client and aggregator in our convention are requests of greatness speedier than existing work. Along these lines, our convention can be connected to an extensive variety of portable detecting frameworks with different scales, plaintext spaces, collection burdens and asset limitations. In light of the Sum conglomeration convention, we additionally proposed two plans to infer the Min total of time-arrangement information. One plan can acquire the exact Min while the other one can get a rough Min with provable lapse ensure at much lower expense.

REFERENCES:-

[1] N. D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A. Doryab, E. Berke, T. Choudhury, and A. Campbell, "Bewell: A smartphone application to monitor, model and promote wellbeing," in 5th International ICST Conference on Pervasive Computing Technologies for Healthcare, 2011.

[2] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G.-S. Ahn, and A. T. Campbell, "The bikenet mobile sensing system for cyclist experience mapping," in Proceedings of the 5th international conference on Embedded networked sensor systems (SenSys), 2007, pp. 87–101.

[3] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, and P. Boda, "Peir, the personal environmental impact report, as a platform for participatory sensing systems research," in Proceedings of the 7th international conference on Mobile systems, applications, and services, ser. MobiSys '09, 2009, pp. 55–68.

[4] T.-H. H. Chan, E. Shi, and D. Song, "Privacy-preserving stream aggregation with fault tolerance," Financial Cryptography and Data Security (FC), 2012.

[5] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, "Vtrack: accurate, energy-aware road traffic delay estimation using mobile phones," in Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, ser. SenSys '09, 2009, pp. 85–98.

[6] S. Consolvo, D. W. McDonald, T. Toscos, M. Y. Chen, J. Froehlich, B. Harrison, P. Klasnja, A. LaMarca, L. LeGrand, R. Libby, I. Smith, and J. A. Landay, "Activity sensing in the wild: a field trial of ubifit garden," in Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems (CHI), 2008, pp. 1797–1806.

AUTHORS :

Mr.B.NarendraStudying II M.Tech (CSE) in St. Ann's College of Engineering & Technology, Chirala,He completed B.Tech.(CSE) in 2012 in Chalapathi Institute of Technology,Guntur.

Mr.AVSSudhakarRaois presently working as Associate Professor, Department of Computer science & Engineering in St. Ann's College of Engineering and Technology, Chirala.He Completed M.Tech. in CSE. He guided many U.G. & P.G projects. He has 10 Years of TeachingExperiance. He published 2 International Journal and presented 1 papers in Internationalconferences.