Scientific Journal Impact Factor (SJIF) : 4.364
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

SECURE TRANSMISSION OF DATA OVER INTERNET USING ELGAMMAL ALGORITHM

PATHMINI C[1], REKHA P[2], SANGEETHA B[3] AND BALAKRISHNAN C[4]
[1,2,3]*Computer Science and Engineering, S.A.Engineering College*
[4]*Associate Professor, S.A.Engineering College*

Abstract-The problem's security necessities of system is knowledge and user privacy goals. It aims to attain the goals, and to strike a balance between coherence and utility, we tend to arrange an economical science construction and its proxy-based variant. These schemes square measure secure within the semi-honest model. The most objective for the constructions and their malicious variants is to originate 2 secret writing functions. {They square measure|they're} tightly coupled within the manner of the 2 functions are independent and one public-key secret writing has an accompaniment similarity. This can be referred to as double secret writing theme. The analysis of the machine and revelation complexities of this construction.It is way more economical than the prevailing protocols. This aggregation protocol has linear quality in estimation and revelation with relevance the amount of users within the system. The quality of spherical is additionally referred to as linear within the range of users. Finally, the aggregation protocol is with efficiency remodeled into a muscular protocol secure within the presence of cruel adversaries, and supply the ensuing protocol's performance and security analysis.

Keywords-Network traffic distribution, Data aggregation, Privacy preservation, malicious security, Smart grid, Data privacy, big data, and multiple clouds

I. INTRODUCTION

The problem of computing the over-threshold parts, parts whose count is bigger than a given worth, in a very personal manner is of specific interest in several applications. A typical application that involves such primitive is network traffic distribution, wherever n network sensors have to be compelled to put together analyze the protection alert broadcasted by completely different sources so as to seek out potential suspect sites. In such application, and while not losing generality, every of such sensors contains a set of suspects and would love to collaboratively cipher the foremost frequent parts on every of those sets (e.g., the count larger than , spoken as +) while not revealing the set of suspects to alternative sensors with whom she collaborates. Formally, let there be n users denoted by ui; one i n, and every of them contains a personal multiset Xi of cardinality k. For simplicity, assume that every of the multisets has a similar cardinality. personal + Aggregation downside. Let ; 2 N, and for a collection X and a pair of X, let F( ) denote the quantity of frequencies (or occurrences) of in X. Then the matter at hand is outlined as follows: given n multisets of cardinality k, realize a collection Z = f 1; : : : ; g U = Sn i=1 Xi specified (i) for all parts two U, if has the multiplicity larger than or adequate to , then 2 Z, i.e., Z = n two [ni =1Xi F ( ) o ; (ii) no polynomial-time rule will learn any component aside from the output of a + protocol, and (iii) no polynomial-time rule ought to apprehend that output of the execution belongs to that user . As recognized in employing a trustworthy third party (TTP) to unravel the personal + aggregation downside is impractical since it's onerous to seek out such entity in several settings. Also, victimisation secure multiparty computations (SMC) is impractical since they're computationally dear. A final approach is to use existing personal set-operation protocols like particularly multiset union protocols. These protocols firmly cipher all parts showing within the union of input multiset specially permits to seek out all parts whose multiplicity is a minimum of . Since these protocols provide associate

output as a collection, the output doesn't have the multiplicity data. whereas this feature will be useful from a privacy stance, it risks the practicality of applications looking forward to the multiplicity of parts, as well as + aggregation.

II. SURVEY ON SECURE TRANSMISSION OF DATA OVER INTERNET USING ELGAMMAL ALGORITHM.

M. Burkhart and X. Dimitropoulos [1] " Fast Privacy-Preserving Top-*k* Queries using Secret Sharing" The ton of analysis has centered on distributed top-*k* computation.A set of parties hold non-public lists of key-value pairs and need to search out and disclose the *k* key-value pairs with largest mixture values while not revealing the other info. It uses secure multiparty computation (MPC) techniques to unravel this downside and style 2 MPC protocols, PPTK and PPTKS, putt prominence on their potency. Proof of plain text information uses a hash table to precipitate a probably massive and distributed house of keys and to probabilistically estimate the mixture values of the top-*k* keys. PPTKS uses multiple hash tables, to enhance the estimation accuracy of PPTK.

S. Bayer and J. Groth [2] "Efficient Zero-Knowledge Argument for Correctness of a Shuffle" In e-voting schemes and different applications that need uncertainty Shuffles of homomorphic encryptions area unit typically utilized in the development of mix-nets. A shuffle permutes and reencrypts a collection of ciphertexts, however because the plaintexts area unit encrypted it's insufferable to verify directly whether or not the shuffle operation was done properly or not. Therefore, to prove the correctness of a shuffle it's typically necessary to use zero-knowledge arguments. we tend to propose AN honest supporter zero-knowledge argument for the correctness of a shuffle of homomorphic encryptions. The urged argument has sublinear communication complexness that's a lot of smaller than the scale of the shuffle itself. additionally the urged argument matches rock bottom computation value for the supporter compared to previous work and additionally has an economical prover. As a result our theme is considerably a lot of economical than previous zero-knowledge schemes in literature. we tend to provide performance measures from AN implementation wherever the correctness of a shuffle of one hundred,000 ElGamal ciphertexts is proved and verified in around a pair of minutes.

Martin Burkhart[3] "SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics" Secure multiparty computation (MPC) permits joint privacy-preserving computations on knowledge of multiple parties. though MPC has been studied well, building solutions that area unit sensible in terms of computation and communication value continues to be a significant challenge. during this paper, we tend to investigate the sensible quality of MPC for multi-domain network security and observation. we tend to initial optimize MPC comparison operations for process high volume knowledge in close to time period. we tend to then style privacy-preserving protocols for event correlation and aggregation of network traffic statistics, like addition of volume metrics, computation of feature entropy, and distinct item count. Optimizing performance of parallel invocations, we tend to implement our protocols beside an entire set of basic operations in a very library known as SEPIA. we tend to measure the period and information measure needs of our protocols in realistic settings on a neighborhood cluster moreover as on PlanetLab and show that they add close to time period for up to a hundred and forty input suppliers and nine computation nodes. Compared to implementations exploitation existing all-purpose MPC frameworks, our protocols area unit considerably quicker, requiring, for instance, three minutes for a task that takes two days with all-purpose frameworks. This improvement paves the method for brand spanking new applications of MPC within the space of networking. Finally, we tend to run SEPIA's protocols on real traffic traces of seventeen networks and show however they supply new potentialities for distributed troubleshooting and early anomaly detection.

Chow and J.-H. Lee [4] " Two-Party Computation Model for Privacy-Preserving Queries over Distributed Databases" Many existing privacy-preserving techniques for querying distributed databases of sensitive info don't scale for big databases as a result of the employment of heavyweight scientific discipline techniques. additionally, several of those protocols need many rounds of interactions between the participants which can be impractical in wide-area settings. At the opposite extreme, a trustworthy party primarily based approach will give quantifiability however it forces the individual databases to reveal non-public info to the central party. This paper shows the way to perform numerous privacypreserving operations in a very ascendable manner below the honest-but-curious model. Our system provides constant level of quantifiability as a trustworthy central party primarily based resolution whereas providing privacy guarantees while not the requirement for heavyweight cryptography. The key plan is to develop an alternate system model employing a Two-Party question Computation Model comprising of a randomizer and a computing engine that don't reveal any info between themselves. we have a tendency to conjointly show however one will replace the randomizer by a light-weight key-agreement protocol. we have a tendency to formally prove the privacy-preserving properties of our protocols and demonstrate the quantifiability and utility of our system employing a real-world implementation.

Taher Elgamal[5] "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" A new signature theme is planned, along side associate implementation of the Diffie-Hellman key distribution theme that achieves a public key cryptosystem. The protection of each system depends on the problem of computing distinct logarithms over finite fields.

Qinghua Li and Guohong Cao[6] " Efficient Privacy-Preserving Stream Aggregation in Mobile Sensing with Low Aggregation Error" Aggregate statistics computed from time-series knowledge contributed by individual mobile nodes are often terribly helpful for several mobile sensing applications. Since the information from individual node is also privacy-sensitive, the individual ought to solely learn the required statistics while not compromising the privacy of every node. To supply sturdy privacy guarantee, existing approaches add noise to every node's knowledge and permit the individual to induce a loud total combination. However, these approaches either have high computation price, high communication overhead once nodes be a part of and leave, or accumulate an oversized noise within the total combination which implies high aggregation error. During this paper, we have a tendency to propose a theme for privacy-preserving aggregation of time-series knowledge in presence of untrusted individual, that provides differential privacy for the total combination. It leverages a unique ring-based interleaved grouping technique to with efficiency cope with dynamic joins and leaves and succeed low aggregation error. Specifically, once a node joins or leaves, solely atiny low range of nodes ought to update their scientific discipline keys. Also, the nodes solely conjointly add atiny low noise to the total to confirm differential privacy, that is O(1) with relevancy the quantity of nodes. supported symmetric-key cryptography, our theme is incredibly economical in computation.

Ms. Shubhangi D. Patil, Dr. S. C. Mehrotra [7] "A Verifiable Secret Shuffle of Homomorphic Encryptions 2010" We show the way to prove in honest friend zero-knowledge the correctness of a shuffle of homomorphic encryptions (or homomorphic commitments.) A shuffle consists during a arranging of the input ciphertexts and a reencryption of them so the permutation isn't unconcealed. Our theme is a lot of economical than previous schemes each in terms of communication quality and machine quality. Indeed, within the case of shuffling ElGamal encryptions, the proof of correctness is smaller than the encryptions themselves.

Yao-Chung Fan and Arbee L.P. Chen[8] " Efficient and Robust Schemes for Sensor Data Aggregation Based on Linear Counting" 2011 Sensor networks have received sizable attention in recent years, and area unit typically used within the applications wherever knowledge area unit tough or costly to gather. In these applications, additionally to individual sensing element readings, applied

mathematics aggregates like Min and Count over the readings of a bunch of sensing element nodes area unit typically required. To conserve resources for sensing element nodes, in-network methods area unit adopted to method the aggregates. One primitive in-network aggregation strategy is that the tree-based aggregation, wherever the aggregates area unit computed from leaves to the foundation of a spanning tree over a sensing element network. However, a defect with the treebased aggregation is that it's not sturdy against communication failures, that area unit common in sensing element networks. one amongst the solutions to beat this defect is to alter multipath routing, by that every node broadcasts its reading or a partial combination to multiple neighbors. each schemes offer an equivalent accuracy guarantee however involve totally different communication prices. Through intensive experiments with real-world and artificial knowledge, we tend to demonstrate the potency and effectiveness of victimisation these 2 schemes as solutions for process aggregates in a very sensing element network. The experiments additionally show that the theme that dynamically allocates the area typically outperforms the opposite one in terms of energy conservation since it needs less area to satisfy associate accuracy constraint.

Ximeng Liu [9] "Privacy-Preserving Patient-Centric Clinical Decision Support System on Naive Bayesian Classification" Clinical call network, that uses advanced data processing techniques to assist practitioner build correct selections,has received significant attention recently. The advantagesof clinical call network embrace not solely up identification accuracy however additionally reducing identification time. Specifically, withlarge amounts of clinical information generated everyday, naive Bayesian classification will be utilised to excavate valuable info to improve a clinical call network. Though the clinical call network is kind of promising, the flourish of the systems till faces several challenges as well as info security and privacy issues. During this paper, we tend to propose a replacement privacy-preserving patient-centric clinical call network, that helps practitioner complementary to diagnose the chance of patients' malady in an exceedingly privacy-preserving method. within the planned system, the past patients' historical information area unit hold on in cloud and might be accustomed train the na¨ıve theorem classifier while not leaky a person patient medical information, so the trained classifier will be applied to figure the malady risk for brand new returning patients and additionally permit these patients to retrieve the top-k malady names in line with their own preferences. Specifically, to guard the privacy of past patients' historical information, a replacement cryptographical tool referred to as additive homomorphic proxy aggregation theme is intended. Moreover, to leverage the leak of na¨ıve theorem classifier, we tend to introduce a privacy-preserving top k malady names retrieval protocol in our system. Elaborated privacy analysis ensures that patient's info is personal and cannot be leaked out throughout the malady identification part. Additionally, performance analysis via in depth simulations additionally demonstrates that our system will with efficiency calculate patient's malady risk with high accuracy in an exceedingly privacy-preserving method.

Qian Wang, Member, IEEE[10] "Real-time and Spatio-temporal Crowd-sourced Social Network Data Publishing with Differential Privacy " Nowadays large crowd-sourced information from mobile devices became wide accessible in social networks, enabling thepossibility of the many vital data processing applications to enhance the standard of our daily lives. Whereas providing tremendous edges, the release of crowd-sourced social network information to the general public can cause goodish threats to mobile users' privacy. During this paper, we investigate the matter of period of time spatio-temporal information business enterprise in social networks with privacy preservation. Specifically, weconsider continuous publication of population statistics and style RescueDP - a web combination observation framework over infinitestreams with w-event privacy guarantee. Its key elements together with reconciling sampling, reconciling budget allocation, dynamicgrouping, perturbation and filtering, area unit seamlessly integrated as a full to supply privacy-preserving statistics business enterprise on infinitetime stamps. Moreover, we tend to more propose associate degree increased RescureDP with neural networks to accurately predict the values of statistics and improve the utility of free information.

Each RescueDP and also the increased RescueDP area unit proved satisfying w-event privacy. We evaluate the planned schemes with real-world moreover as artificial datasets and compare them with 2 w-event privacy-assured representative ways. Experimental results show that the planned schemes surmount the prevailing ways and improve the utility of period of time information sharing with robust privacy guarantee.

Kun Ma, Han Liang, and Kaijie Wu [11] "Homomorphic Property-Based Concurrent Error Detection of RSA:A Countermeasure to Fault Attack" Fault-based attacks, that recover secret keys by deliberately introducing fault(s) in cipher implementations and analyzing the faulty outputs, are proven to be very powerful. During this paper, we have a tendency to propose a completely unique synchronal Error Detection (CED)scheme to counter fault-based attack against RSA by exploiting its increasing homomorphic property. Specifically, the planned CED theme verifies if _ki¼1EðmiÞ nine Eð_ki¼1mi mod nÞ ðmod nÞ wherever E might be either RSA secret writing, or decoding, or signature, or verification method. Upon a couple, all the ciphertexts are going to be suppressed. The time overhead is 1=k and k will be accustomed trade-off the time overhead with memory overhead and output latency. Recognizing that associate degree RSA device might be subject to a mixture of several side-channel attacks, the planned theme allows a straightforward divide-and-concur solution—any fine-tuned design, for example, a power-attack-resistant design, will be equipped with fault-attack resistance simply while not worrying its original resistance. This advantage distinguishes the planned theme over the prevailing countermeasures.

III. CONCLUSION

The development of 2 protocols, with variable operation overhead, analyzed their security, and incontestible their utility by analyzing its precise procedure and communicative value. Moreover, we tend to provide a full proof showing that our protocol is secure within the presence of semi-honest adversaries. Since the semi-honest protocols usually have essential security restrictions, by requiring each person to follow the directions laid out in the protocol, we tend to remodeled our basic protocol into a stronger + protocol that is additionally secure within the presence of malicious adversaries. Additionally to a full description of our protocol with malicious adversaries, we tend to proven that the protocol is secure at intervals the simulation paradigm. Within the future, we are going to look at changing the Zero-Knowledge Proofs from their gift interactive variant into Non-Interactive Zero information Proofs through the Fiat-Shamir heuristic, which can improve the communication quality of our protocols.

REFERENCES

[1] M. Burkhart, X. Dimitropoulos," Fast privacy-preserving top-k queries using secret sharing", In IEEE ICCCN, 2010.
[2] S. Bayer,J. Groth," Efficient zero-knowledge argument for correctness of a shuffle" In D. Pointcheval and T. Johansson, editors, Advances in Cryptology-Eurocrypt, LNCS 7237, pages 263–280, 2012.
[3] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos." SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics", In USENIX Security, 2010.
[4] S. Chow and J.-H. Lee and L. Subramanian." Two-party computation model for privacy-preserving queries over distributed databases", In NDSS, 2009.
[5] T. El Gamal," A public key cryptosystem and a signature scheme based on discrete logarithms", In G. R. Blakley and D. Chaum, editors, Advances in Cryptology-Crypto, LNCS 196, pages 10–18, 1984.
[6] Q. Li and G. Cao, "Efficient and privacy-preserving data aggregationin mobile sensing," in Proc. Int. Conf. Netw. Protocols, 2012,pp. 1–10
[7] C. Neff, "A verifiable secret shuffle and its application to evoting",in Proc. ACM Conf. Comput.Commun. Security, 2001,pp. 116–125.
[8] Y.-C. Fan and A. L. P. Chen, "Efficient and robust schemes for sensor data aggregation based on linear counting", IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 11, pp. 1675–1691, Nov. 2010.

[9] Ximeng Liu, *Student Member*, *IEEE*, Rongxing Lu, *Member*, *IEEE*, Jianfeng Ma, Le Chen, and Baodong Qin," Privacy-Preserving Patient-Centric Clinical Decision Support System on Na¨ıve Bayesian Classification".

[10] Qian Wang, Member, IEEE, Yan Zhang, Xiao Lu, Zhibo Wang, Member, IEEE, Zhan Qin, Student Member, IEEE, and Kui Ren, Fellow, IEEE ,"Real-time and Spatio-temporal Crowd-sourced Social Network Data Publishing with Differential Privacy"

[11] Kun Ma, Han Liang, and Kaijie Wu, Member, IEEE Homomorphic Property-Based Concurrent Error Detection of RSA:A Countermeasure to Fault Attack".