IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 33, No. 1, February, 2019, pp. 53-60
Journal homepage: http://iieta.org/journals/ria

An Efferent and Secure Outsourced Data Aggregation Using Location Sharing Services

Thulasi Bikku

Department of Computer Science & Engineering, Vignan's Nirula Institute of Technology & Science for Women, PedaPalakaluru, Guntur-522 005, Andhra Pradesh, India

Corresponding Author Email: thulasi.jntuk@gmail.com

https://doi.org/10.18280/ria.330110

Received: 12 January 2019
Accepted: 5 February 2019

Keywords:
location privacy, broadcast encryption, vector commitments, selective total, differential protection, RSA calculation, context privacy, source-location privacy, cyber security

ABSTRACT

In the beginning, the web information is structured and facilitated by a solitary individual, gathering, or association. Site pages are progressively made out of substance from cluster irrelevant Location-sharing-based services (LSBSs) enable clients to impart their area to their companions in a sporadic way. In the present conveyed LSBSs clients must unveil their area to the specialist organization so as to impart it to their companions. The moderating up of bits is additionally done to guarantee the security at the vehicle layer level in seeking. The unwavering quality and security of the protection is high on utilizing RSA algorithm for Encryption. Diverse security objectives must be accomplished new convention is ideal tradeoffs in various security objectives and vitality utilization. Centering imperative sort of security, a new strategy is proposed in written works, self-modifying apparition steering is an extremely effective one. However, despite everything it has a few limitations, but it gives better results when compared with existing system. In this paper we propose an improved rendition of it to upgrade its execution. This paper gives a new organized diagram proposals and research bearings of security arrangements use for protection saving meter information conveyance and the executives. Moreover we broaden our plans is specialist service provider, playing out some check work, can gather security saving total insights on the areas clients share with one another.

1. INTRODUCTION

The term shrewd network is utilized comprehensively to allude the up and coming age of electrical vitality transmission and conveyance foundations to portray by a tight joining with Information and Communication Technologies (ICT). The reconciliation of the power framework with ICT will empower inescapable continuous observing of the physical procedures, including age and utilization at the clients' premises just as ongoing control activities, including controlling the conduct of brilliant machines for interest reaction [1]. One of most evident provokes seeming to undermine the effective arrangement of sensor systems is the worry of security accomplishing protection in sensor systems is a confounded issue by the way that sensor organizes regularly comprise of a lot of minimal effort radio gadgets that work on promptly accessible, institutionalized remote correspondence advances [2].

There has been a sensitive development in the measure of information accessible on organized Personal Computers around the globe, quite a bit of it as characteristic language reports. An expanding assortment of internet indexes exist for recovering such archives in view of coordinating catchphrases [3].

Be that as it may, accuracy of retrieving only useful text is regularly imperfect—it is very frequently still an agonizing mission for a client to attempt a few hunt questions and read various archives before a required snippet of knowledge is found [4]. Information accumulated by a hub from the checked field is sent to the base station through different bounces other than these, sensor hubs may likewise have application subordinate extra segments. LSBSs license clients to impart their present area or action to other individuals [5].

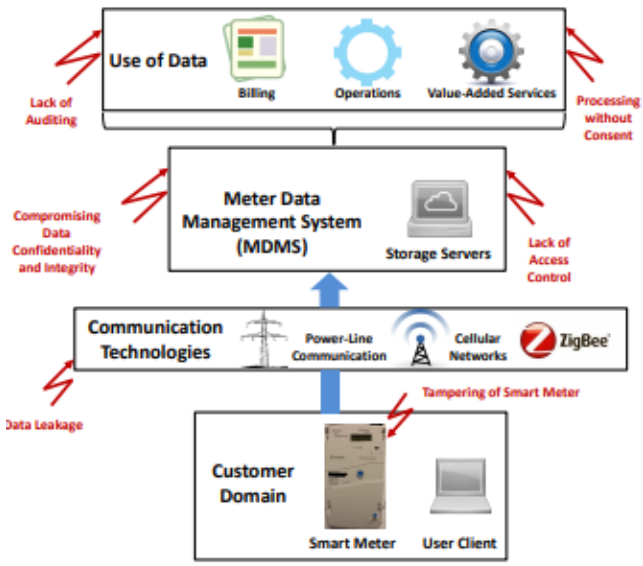

Figure 1. Overview of threats in the smart metering infrastructure

In the Figure 1, the user or customer domain contains smart meter and user client, a smart meter is a gadget which distinguishes power utilization and other data to a relating

utility for checking and charging purposes. The meters speak with the line and utility frameworks by means of a concentrated headend, called AMI (advanced metering infrastructure). The AMI interfaces with expansive quantities of shrewd meters so as to serve huge locale [6]. Utilizing indistinguishable propelled techniques from web banking and ATM machines, computerized smart meters encode (code) clients' vitality utilization information to guarantee protection, transmitting it to the utility over a remote system with different layers of security joined all through the framework. The execution of safety efforts is tried and looked into normally to make preparations for unapproved access to frameworks. The common area information might be as Global Positioning System (GPS) facilitates, despite the fact that in Geo Social Networks (GSN) their area in an all the more socially significant path by giving the setting [7]. The approach part opens by exploring why outsider web following offers ascend to protection concerns and manners by which arrangement may be organized to address those worries.

This decreases the expense of a LSBS supplier that is then ready to offer its administration at a lower cost if seeking after a membership based plan of action. Moreover we expand our plans with the end goal that the specialist service provider can gather security protecting insights on the areas shared by the clients [8].

Modern internet technology has collapsed geographical boundaries for global information sharing. Outsourcing has been an important and increasing driving force for global information sharing. It involves transferring or sharing management control of a business function to an outside supplier and involves information exchange among the service providers and outsourcing clients. One of the most notable outsourcing services is database outsourcing where organizations outsource the data storage and management to third-party service providers [9].

Traditionally, information integration in both industry and research has assumed that information in each database can be freely shared. It is widely recognized today that data confidentiality and privacy are increasingly becoming an important aspect of data sharing and integration because organizations or individuals do not want to reveal their private databases for various legal and commercial reasons. The structure of data aggregation is depicted in the Figure 2. In the Outsourced Data Aggregation (ODA), associations re-appropriate their information the board needs to an outer specialist service provider. The service provider has customer's databases and offers consistent instruments to make, store, update and access their databases. This model acquaints a few research issues related with information security which we investigate. The Outsourced Database Aggregation comprises of 3 elements: (1) the information owner(s), (2) the database service providers (server) and (3) the client(s). The information proprietor makes, changes and erases the substance of the database. The server has the proprietor's database, i.e., the proprietor re-appropriates its database to the server. The customer's issue inquiries about the database to the server. A portion of the parameters recognizing a particular ODA incorporates the number of proprietors and customers and the kind of trust in the server. These range from providing data confidentiality, authenticity and integrity, to enabling an untrusted server to run queries over encrypted data. It includes customers putting away their information at servers managed by possibly untrusted service providers [10]. In spite of the fact that servers are depended upon for the administration/organization and accessibility of customers' information, they are commonly not trusted with the real information substance. In this defining, the primary security objective is to limit the measure of data about the information that the server can infer, while as yet enabling the last to execute inquiries over scrambled databases [11].

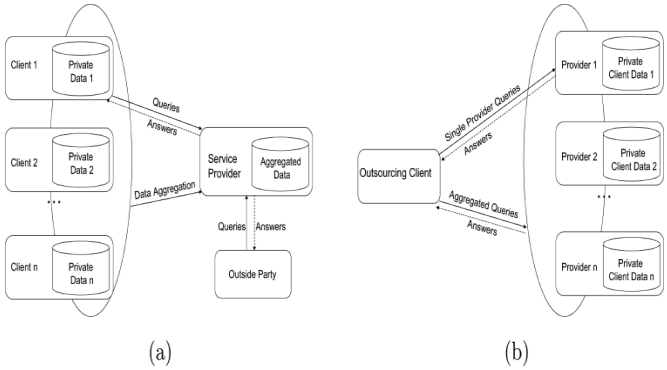

Figure 2. (a) Data aggregation service provider (b) Client outsourcing

2. LITERATURE SURVEY

We audit muddling based Location Privacy Preserving Mechanisms (LPPMs) and contend that they are not appropriate for securing area protection in LSBSs. Accordingly some of them have been intentionally intended for ensuring area security in LSBSs; others have an increasingly broadly useful [12].

While LSBSs are in reality valuable, the exposure of location information raises significant security concerns. Service providers of data and other outsiders with access to exact area information can surmise private client data, for example, their development designs, personal residence, way of life and interests [8]. Further, making these derivations is significantly simpler if clients share the location instead of simply submitting coordinates and directions, as any vulnerabilities presented by conceivable mistakes in the GPS arranges are expelled. We note that, in spite of the fact that GSNs offer congurable protection settings, they are as yet security obtrusive, as the LSBS supplier learns the clients' area paying little heed to the security settings.We thusly pursue the classification which recognizes these four jumbling techniques: area concealing, irritation, including sham areas, and lessening accuracy [11].

Conveyed differential protection is created in this paper to empower the examination and it registers scale rate Cluster based Private Data Aggregation (CPDA) is utilized chiefly for lessening computational overheads [13]. The down to earth systems build up the equipment and programming based methodologies over the encoded information and furthermore it gives the code impression in the confided in condition.

Bailey et al. [14] has proposed Vision-based Web Entity Extraction utilizing VIPS (VIsion-based Page Segmentation) Algorithm. The VIsion-based Page Segmentation (VIPS) algorithm aims to extract the semantic structure of a web page based on its visual presentation. Label trees will in general spotlight on the introduction structure rather than the substance structure which is the fundamental issues with past fills in as they frequently are not right enough to separate in the site page the semantic segments. Likewise planners have distinctive style to make a site page which is perplexing and

shifted. This paper proposes Vision-based page division way to deal with dealing these issues. It does the page division dependent on human discernment and utilizations different page design highlights like text dimension, distinctive hues utilized in the areas of a site page to construct a dream tree for a page. It is not concentrating on external parameters like user inputs or functional scripts.

Liao et al. [15] has presented a Hierarchical Conditional Random Field method for understanding a page format. To get proficient and precise outcomes on data recovery of substances the significance of Page-format understanding is a flat out need. With Vision-tree, hubs are the resultant yield yet doling out the marks turns into an errand. It incorporates the long separation conditions to accomplish promising outcomes. Recognizable proof of substance is a standout amongst the most critical element data recovery. To get required data for the predetermined inquiry must be considered if the elements are very much characterized.

William W. Cohen et al. [16] has presented semi-Markov conditional random field (CRF) in which as per the appointed names the text substance inside the html component is portioned to distinguish the elements substantially better and precise way. Additionally the yield is exhaustive depiction about the substances as entire together.

Jones et al. [17] have displayed Geographic data Extraction from web records and text information. They have created Game theroretic frameworks which encourage associations and organizations to extricate and addresses from their web areas. The estimations of Recall measures, Precision and F-measure show promising outcomes. In this way these empowering results can be considered for the few issues looked in geological data recovery methods.

Shabtai et al. [18] arranged wrappers into four distinctive classes, including hand-made wrappers utilizing general programming dialects, extraordinarily composed programming dialects or devices, heuristic-based wrappers, and wi-fi (WI) approaches.

Akkus et al. [19] took after this scientific classification and thought about WI frameworks from the client perspective and segregated infrared (IR) apparatuses in view of the level of robotization. They characterized IR apparatuses into four distinctive classes, including frameworks that need developers, frameworks that need explanation illustrations, comment free frameworks and semi supervised frameworks.

Song et al. [20] who keeps up the rise of the internet page, grouped IR apparatuses into three unique classes as indicated by the kind of information reports and the structure/imperatives of the retrieval designs. The top notch incorporates instruments that procedure IR from free text utilizing retrieval designs that are primarily in view of syntactic/semantic imperatives.

In open key cryptosystems, bootstrapping is certifiably not a good arrangement as a result of asset poor sensor hubs Elliptic-curve cryptography (ECC) is in this way utilized for setting up group keys utilizing evident mystery sharing on account of its littler keys capacity to figure quick and need of lesser assets like diminished space, data transmission and preparing power [21]. We propose changes dependent on the settled K-obscurity idea to figure careful responses for range and closest neighbor look, without uncovering the question source the protection mindful inquiry processor restores a competitor rundown of answers in which the precise inquiry answer to the client issuing the question through the location anonymizer must be incorporated.

3. SYSTEM ARCHITECTURE

The client needs to enroll with the username and secret word, the information will be secure in the database. This database will be kept up by an administrator. The administrator transfers the items. When the record is made, the client can login and scan for catchphrases. This contrasts from our work in that we center around venue sharing, and not on choosing where to meet after a gathering of clients has purposely chosen to do as such [22]. This convention clients will not reveal their location to different clients a few works utilize Private Information Retrieval (PIR) with the goal that the clients recover data identified with their surroundings [23]. This is just span in which there are no odds of any sort of assault. Subsequent to observing the conduct of different hubs in a similar zone, every sensor hub figures the notoriety esteem for them.

Once a node determines which points in its private database are among the k-nearest neighbors of the query instance based on the k-nearest distances, the second step is to determine the global classification based on the local classifications. Each of these neighbors is supposed to vote in favor of its own class, with the strength of the vote determined by its distance to x. All the votes are then added and the class with the highest votes is selected as the classification of x. In order to minimize the disclosure of individual classification information, we can represent the local classification of x as a vector of v votes, assuming the number of classes is v. The i^{th} element of this vector is the amount of votes the i^{th} class received from the points in this node's database which are among the k-nearest neighbors of x. Then we can add these local classification vectors by a simple privacy-preserving addition protocol to determine the global classification vector [24]. Once each node knows the global classification vector, it can determine the classification of x without disclosing its local classifications.

We characterize the security properties that a protection safeguarding LSBS ought to satisfy and propose two developments. Initial, a development dependent on Identity Based Broadcast Encryption (IBBE) in which the specialist organization does not get familiar with the client's location, yet realizes which different clients are permitted to get an area update. Second, a development dependent on mysterious IBBE in which the specialist service provider does not gain proficiency with the last either. As favourable circumstances as for past work, in our plans the LSBSs supplier does not have to play out any activities to figure the answer to an area information demand, however just needs to advance IBBE ciphertexts to the recipients [25].

The classification of data is performed using the algorithm represented below

Algorithm:

INPUT: x

OUTPUT: $classification(x)$

Each node computes the distance between x and each point y in its database, $d(x, y)$, selects k smallest distances (locally), and stores them in a local distance vector ldv.

(1). Using ldv as input, the nodes use the PrivateTop$k$ protocol to select k nearest distances (globally), and stores them in gdv.

(2). Each node selects the k^{th} nearest distance = $gdv(k)$.

(3). Assuming there are v classes, each node calculates a local classification vector lcv for all points y in its database:

(4). $\forall 1 \le i \le v$, $lcv(i) = y\ w(d(x, y))* [f(y) == i]$ && $[d(x, y) \le y]$, where $d(x, y)$ is the distance between x and y, $f(y)$ is the classification of point y, and $[p]$ is a function that evaluates to 1 if the predicate p is true, and 0 otherwise.

(5). Using *lcv* as input, the nodes use a privacy preserving addition protocol to calculate the global classification vector *gcv*.

(6). Each node classifies x as $classification(x) \leftarrow \max i \in V\ gcv(i)$.

The diagrammatic representation of the algorithm is executed in the system model shown in the Figure 3.

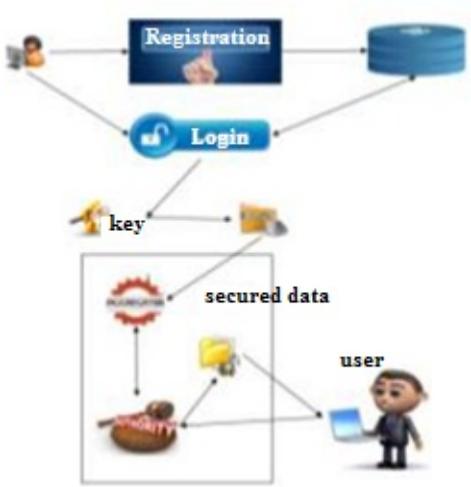

Figure 3. Proposed system model

The information accumulation and control usefulness of computerized meters is accordingly a subset of that of smart meters, as is the arrangement of security issues identified with mechanized meters a subset of the issues identified with smart meters and frameworks took off in many nations record and can transmit estimation information at interims of around 15 minutes yet hourly and day by day detailing are normal.

These three sorts of purposes vary fundamentally regarding their prerequisites on metering recurrence and precision, as far as the number and areas of buyers whose information are required, and as far as the partners. The proposed procedures can essentially decrease the message overhead without losing any inquiry protection.

Managed based techniques for named element acknowledgment for the most part fill in as takes after: an arrangement of guidelines is either physically characterized or naturally learned [28]. Every token in the text is spoken to by an arrangement of components. The text is then looked at against the views and a manage is terminated if a match is found. An administer comprises of a sample and an activity. A sample is typically a general articulation characterized over elements of tokens. At the point when this sample coordinates an arrangement of tokens, the predefined activity is let go. An activity can be marking an arrangement of tokens as a substance, embeddings the begin or end name of an element, or recognizing various elements at the same time. For instance, to name any arrangement of tokens of the frame "Mr. X" where X is an uppercase word as a man element, the accompanying guideline can be characterized:

(token="Mr." orthography sort=FirstCap) → individual name.

Later on we will address different issues, for example, unknown source, key administration, and investigate other inquiry methods to adjust the tradeoff between question postponement and message overhead. This convention gives information respectability and privacy to collection of information progressively encoded with various keys. Various leveled information accumulation is accomplished utilizing message authentication codes (MAC) and protection homomorphism encryption conspire. A few outsiders have JavaScript libraries and Application programming interfaces (APIs) that speed website page stacks and empower new page usefulness [29]. The communication in the Smart Meter, the smart meter acts as traffic generator assigned with a global IPv6 address, receives demand response data from the collector. The Router takes the responsibility of relaying packets from both smart meters and collectors. determines the next hop for the packet to reach the final destination. The collector serves interconnection between a NAN and a WAN in the SG and aggregates all meter reading information. The collector node collects all meter reading data and sends acknowledgement back to corresponding meters, shown in the Figure 4. NANs are supposed to cover large geographical areas where the user and/or field devices are distributed. To cover large geographical devices for communication purposes generally traditional infrastructure based networks such as Wi MAX (Worldwide Interoperability for Microwave Access) or 3G/4G based standards such HSPA (High Speed Packet Access) or LTE (Long Term Evolution) based networks are preferred. Smart meter Act as router for Home Area Network HAN supporting bi-directional Demand management [26].

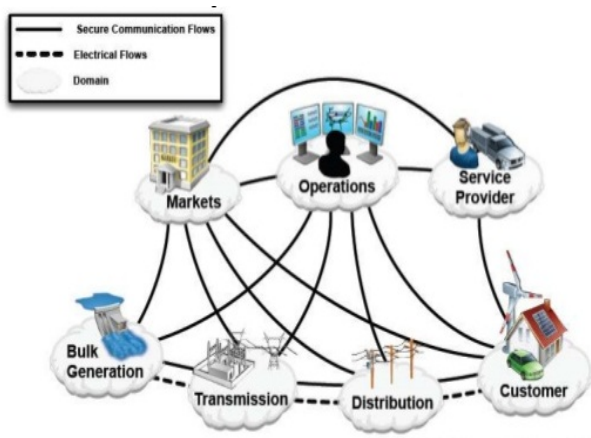

Figure 4. OSS layer for smart meter

4. CONSTRUCTIONS OF LSBS

Our plans depend on personality based communicate encryption the sender private plan which satisfies the sender protection property the completely private plan, which satisfies both the sender security and the recipient protection properties [27].

4.1 Identity-Based broadcast encryption

Communicate encryption enables a sender to scramble a message m to a lot of collectors S∈[1, n], so no alliance of recipients not in S can decode.

Step 1: Setup (1λ, n, size'). On information the quantity of clients n, the security parameter 1λ, and the most extreme size ' ≤ n of a communicate beneficiary gathering, yield the open key pk and the mystery key sk.

Step 2: Key Gen(i, sk). On info a list i and the mystery key sk, yield a mystery key di for client U

Step 3: Enc(pk, S, m). On info the beneficiary gathering S ∈ [1, n], the open key pk and the message m, yield the ciphertext c.

Step 4: Dec(pk, di, c). On information the open key pk, the mystery key di of client Ui and a ciphertext c, yield m on the off chance that I ∈ S or else the disappointment image ⊥.

In IBBE, a believed key age focus KGC makes the parameters and Figures the mystery keys of the collectors. Note that the mystery key sk permits the unscrambling of each figure content. On the off chance that figure writings c not to uncover the arrangement of collectors S, the communicate encryption conspire is mysterious. The results of the IBBE is shown in the Figures 5 and 6.

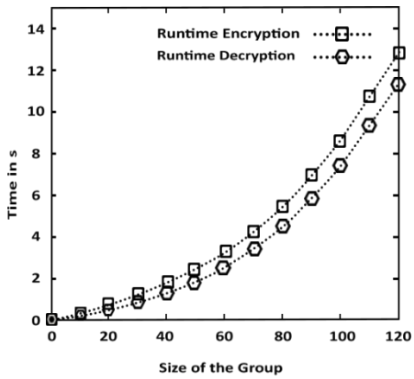

Figure 5. Runtimes for encryption and decryption of IBBE

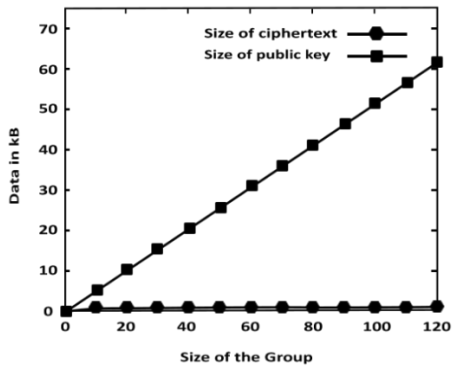

Figure 6. Size of ciphertext and public key in IBBE

4.2 Sender-private LSBS

Our sender-private LSBS (SPLS) utilizes an IBBE plot that is not known. In such a plan, figure writings c contains a portrayal of the beneficiary gathering S. Our plan fills in as pursues:

Step 1: Setup Phase. KGC executes the setup calculation Setup(1λ , n, size') on info the security parameter 1λ , the quantity of clients n and the most extreme size ' ≤ n, distributes the open key pk and stores the mystery key sk. Clients acquire pk.

Step 2: Registration Phase. Every client Ui registers with the specialist service provider by sending the list I. Also, Ui gets the key di from KGC, which runs KeyGen(i, sk).

Step 3: Main Phase. To share an area loc, a client Ui runs c ← Enc(pk, S, i||loc) and sends c to the specialist service provider P. P gets S from c and sends c to the clients Uj (j ∈ S). Every client Uj runs Dec(pk, dj , c) to yield the message i||loc.

We note that the enrollment and principle stages can be interleaved clients can join our SPLS progressively. The IBBE conspire guarantees that no alliance of specialist service provider P and clients U ∈/S can unscramble a figure content c registered on info S this plan does not satisfy the beneficiary security property. Since the IBBE conspire is not known, the figure content c uncovers the character of the recipients Uj (j ∈ S).

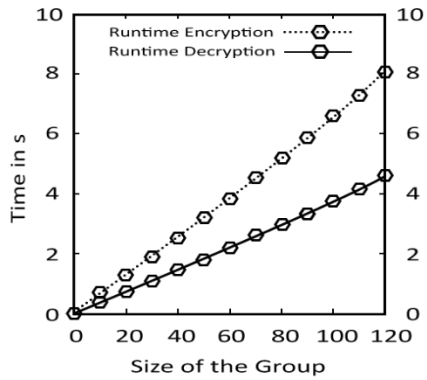

Figure 7. Runtimes for encryption and decryption of SPLS

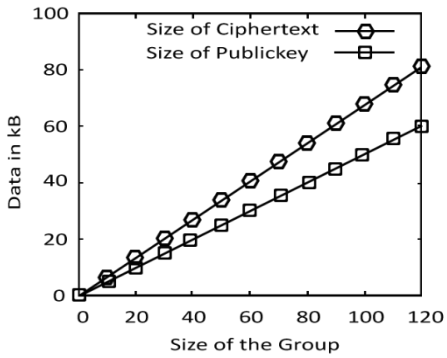

Figure 8. Size of ciphertext and public key in SPLS

The probability model for private data is performed using the below algorithm:

INPUT: gi−1(r), vi

OUTPUT: gi (r)

Pr (r) ← p0 ∗ dr−1

if gi−1(r) ≥ vi then

gi (r) ← gi−1(r)

else

with probability Pr : gi (r) ← a random value between gi−1(r), vi)

with probability 1 − Pr : gi (r) ← vi

end if

4.3 Data encryption and upload

After login the client can begin hunting down catchphrases Homomorphism Rivest–Shamir–Adleman (RSA) method is utilized to encode the pursuit watchword. RSA is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

Generating Public Key:

Select two prime numbers P and Q
Now First part of the Public key: n = P*Q.
We also need a small exponent say e:
But e Must be an integer, not be a factor of n.
$1 < e < \Phi(n)$
The Public Key is made of n and e
Generating Private Key:
We need to calculate $\Phi(n)$ such that $\Phi(n) = (P-1)(Q-1)$
Calculate Private Key, d:
$d = (k*\Phi(n) + 1) / e$ for some integer k

In the wake of scrambling, the encoded information is transferred in the transitional server. The scrambled information will be accessible with the aggregator [23].

For example, convert letters to numbers:
H = (P)8 and I = (Q)9
Thus Encrypted Data c = 89, e mod n.
Thus Encrypted Data comes out to be 1394
Now we will decrypt 1394:
Decrypted Data = cd mod n.
Thus Encrypted Data comes out to be 89
8 = H and I = 9 i.e. "HI".

4.4 Duplicate detection

Instead of simply generating false leaf vertices, the adversary could instead replicate a given reading multiple times. For example, the smallest reading could be replicated many times, causing the median to decrease. The proposed model detects this by first (1) checking whether the committed sequence is sorted and then (2) performing probes on neighboring pairs of values to check for duplicates. The check for sortedness is by repeatedly performing binary searches for uniformly randomly selected elements. It can be known that if there are many out-of-order elements in the committed sequence, the binary search invariant will eventually be violated in the course of one of these searches.

Once we have established that the sequence is mostly sorted with high probability, it is clear that, if there are a substantial number of duplicates, most of these duplicates must occur in-place, i.e., next to the duplicated element so that they do not increase the number of out-of-order elements. Such in-place duplicates are easily detected by unform random sampling of neighboring vertices in the hash tree.

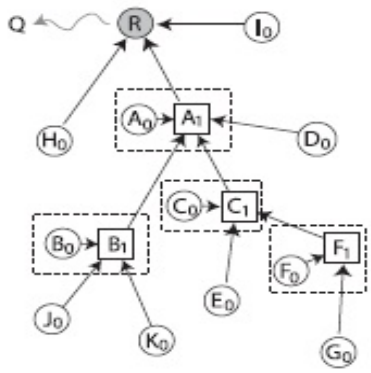

Figure 9. Hash tree

The single aggregator SIA can be extended to support multiple hierarchical aggregators. The simplest extension of the hash tree structure to support multiple aggregators is to have the hash tree follow the topology of the network exactly. The sensor node constructs a leaf vertex consisting of its input value r(G) (e.g., a sensor reading) and its node value G. Each leaf node in the network topology transmits its leaf vertex to its parent (e.g., G sends its leaf vertex to F). The Figure 9 shows the graph structure.

5. PERFORMANCE ANALYSIS

Location sharing-put together applications are generally kept running with respect to a cell phone, for example, an advanced cell or a tablet PC. In this manner the accessible assets at the customer side are restricted as far as computational power and data transmission when on versatile association.

The all out number of clients is in type of diagrams gathered by the category of boys, girls and all. This measurable information demonstrates what number of clients are in on the web and what number of clients are perusing a particular website pages shown in Figure 10.

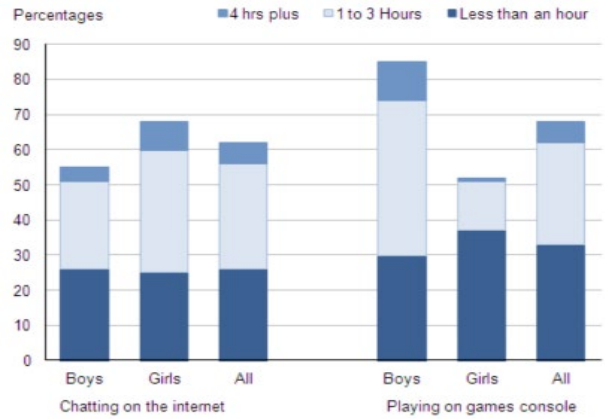

Figure 10. Internet access by various categories

All things are considered, many esteems included administrations would depend contrasting information from various clients, in which case circulated security protecting calculations would be required for actualizing esteem included administrations. Different applications usage provides Location sharing services is shown in Figure 11.

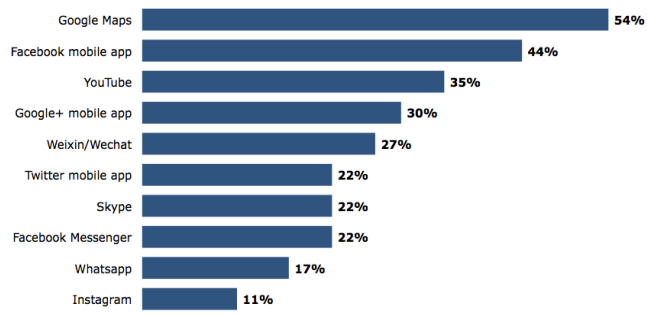

Figure 11. Different applications usage provides Location sharing services

Tending to these issues will require advance in the region of vitality effective and security saving appropriated machine learning methods. Other than area sharing, identification and civic chairman transport conventions are another fundamental usefulness of a GSN. For the last security saving conventions

have been proposed and noted that it is conceivable to join the two ways to deal with construct a protection safeguarding GSN.

6. CONCLUSION AND FUTURE DIRECTIONS

We have overviewed the best in class on smart meter information protection on the three employments of smart meter information, and its security perspectives, we have assessed cryptographic answers for guaranteeing security safeguarding the executives of smart meter information under the believed administrator model, and protection saving answers for information handling under the non-believed administrator display. We note that our schemes are also suitable to implement other services, such as social recommendation applications. This is because in practice users can share arbitrary information in the cipher text. Instead of encrypting location information, users could share their reviews, such as how they like the food in a particular restaurant.

The asset mindful design plans to limit correspondence and computational expense, while the quality-mindful design expects to limit the measure of hidden zones so as to produce progressively precise total areas. We proposed a model joined with the RSA method protection of the client from being in danger and it likewise improves the effectiveness by enabling numerous clients to get associated with a server. As favorable circumstances from past work, in our plans the LSBS supplier does not have to perform complex tasks so as to process an answer for an area information demand, however just needs to advance IBBE figure writings to the beneficiaries. This permits to run a security protecting LSBS at essentially lower costs.

We trust the data introduced here furnishes security and protection scientists with the foundation important to add to this creating field and to seriously take part in the continuous open discussion. Moreover, we expand our plans with the end goal that the specialist organization, playing out some confirmation work, can gather security protecting measurements about the spots clients share among one another.

ACKNOWLEDEMENTS

We extend our sincere thanks to everyone who helped us in the realization of this work and we also thank Chairman of Vignan Institutions. We thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] Whitmore, A., Agarwal, A., Xu, D.L. (2015). The internet of things—A survey of topics and trends. Information Systems Frontiers, 17(2): 261-274. http://dx.doi.org/10.1007/s10796-014-9489-2

[2] Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z. (2017). IoT middleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal, 4(1): 1-20. http://dx.doi.org/10.1109/JIOT.2016.2615180

[3] Witten, I.H., Witten, I.H., Moffat, A., Bell, T.C., Bell, T.C., Bell, TC. (1999). Managing gigabytes: Compressing and indexing documents and images. IEEE Transactions on Information Theory, 41(6): 2101. http://dx.doi.org/10.1109/TIT.1995.476344

[4] Bikku, T. (2018). A new weighted based frequent and infrequent pattern mining method on realtime E-commerce. Ingenierie des Systemes d'Information, 23(5): 121. http://dx.doi.org/10.3166/isi.23.5.121-138

[5] Dong, C., Dulay, N. (2011). Longitude: A privacy-preserving location sharing protocol for mobile applications. In IFIP International Conference on Trust Management, pp. 133-148. http://dx.doi.org/10.1007/978-3-642-22200-9_12

[6] Sankar, L., Rajagopalan, S.R., Mohajer, S. (2013). Smart meter privacy: A theoretical framework. IEEE Transactions on Smart Grid, 4(2): 837-846. http://dx.doi.org/10.1109/TSG.2012.2211046

[7] Batty, M., Axhausen, K.W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Portugali, Y. (2012). Smart cities of the future. The European Physical Journal Special Topics, 214(1): 481-518. http://dx.doi.org/10.1140/epjst/e2012-01703-3

[8] Bilogrevic, I., Jadliwala, M., Kalkan, K., Hubaux, J.P., Aad, I. (2011). Privacy in mobile computing for location-sharing-based services. In International Symposium on Privacy Enhancing Technologies Symposium, pp. 77-96. http://dx.doi.org/10.1007/978-3-642-22263-4_5

[9] Selviaridis, K., Spring, M. (2007). Third party logistics: a literature review and research agenda. The International Journal of Logistics Management, 18(1): 125-150. http://dx.doi.org/10.1108/09574090710748207

[10] Xiong, L., Chitti, S., Liu, L. (2007). Preserving data privacy in outsourcing data aggregation services. ACM Transactions on Internet Technology (TOIT), 7(3): 17. http://dx.doi.org/10.1145/1275505.1275510

[11] Liu, H., Chen, G., Huang, Y. (2017). Smart hardware hybrid secure searchable encryption in cloud with IoT privacy management for smart home system. Cluster Computing, 1-11. http://dx.doi.org/10.1007/s10586-017-1143-6

[12] Herrmann, M., Rial, A., Diaz, C., Preneel, B. (2014). Practical privacy-preserving location-sharing based services with aggregate statistics. In Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks, pp. 87-98. http://dx.doi.org/10.1145/2627393.2627414

[13] Bhasker, L. (2014). Genetically derived secure cluster-based data aggregation in wireless sensor networks. IET Information Security, 8(1): 1-7. http://dx.doi.org/10.1049/iet-ifs.2013.0133

[14] Bailey, D.G., Hodgson, R.M. (1988). VIPS—A digital image processing algorithm development environment. Image and Vision Computing, 6(3): 176-184. http://dx.doi.org/10.1016/0262-8856(88)90024-8

[15] Liao, L., Fox, D., Kautz, H. (2007). Hierarchical conditional random fields for GPS-based activity recognition. Robotics Research, 28: 487-506. http://dx.doi.org/10.1007/978-3-540-48113-3_41

[16] Sarawagi, S., Cohen, W.W. (2005). Semi-Markov conditional random fields for information extraction. In Advances in Neural Information Processing Systems, pp. 1185-1192.

[17] Jones, C.B., Abdelmoty, A.I., Fu, G. (2003). Maintaining ontologies for geographical information retrieval on the web. In OTM Confederated International Conferences"

On the Move to Meaningful Internet Systems", pp. 934-951. http://dx.doi.org/10.1007/978-3-540-39964-3_59

[18] Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., Weiss, Y. (2012). "Andromaly": A behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, 38(1): 161-190. http://dx.doi.org/10.1007/s10844-010-0148-x

[19] Akkus, I.E., Chen, R., Hardt, M., Francis, P., Gehrke, J. (2012). Non-tracking web analytics. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 687-698. http://dx.doi.org/10.1145/2382196.2382268

[20] Song, D.X., Wagner, D., Perrig, A. (2000). Practical techniques for searches on encrypted data. In Proceeding 2000 IEEE Symposium on Security and Privacy, pp. 44-55.

[21] Gura, N., Patel, A., Wander, A., Eberle, H., Shantz, S.C. (2004). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 119-132. http://dx.doi.org/10.1007/978-3-540-28632-5_9

[22] Li, N., Chen, G. (2010). Sharing location in online social networks. IEEE Network, 24(5): 20-25. http://dx.doi.org/10.1109/MNET.2010.5578914

[23] Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T. (2000). Protecting data privacy in private information retrieval schemes. Journal of Computer and System Sciences, 60(3): 592-629. http://dx.doi.org/10.1006/jcss.1999.1689

[24] Xiong, L., Chitti, S., Liu, L. (2007). Mining multiple private databases using a KNN classifier. In Proceedings of the 2007 ACM symposium on Applied Computing, ACM, pp. 435-440. http://dx.doi.org/10.1145/1244002.1244102

[25] Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. In Annual International Cryptology Conference, pp. 213-229. http://dx.doi.org/10.1137/S0097539701398521

[26] García, A.P., Oliver, J., Gosch, D. (2010). An intelligent agent-based distributed architecture for Smart-Grid integrated network management. In IEEE Local Computer Network Conference, pp. 1013-1018. http://dx.doi.org/10.1109/LCN.2010.5735673

[27] Schlegel, R., Chow, C.Y., Huang, Q., Wong, D.S. (2017). Privacy-preserving location sharing services for social networks. IEEE Transactions on Services Computing, 10(5): 811-825. http://dx.doi.org/10.1109/TSC.2016.2514338

[28] Vejendla, L.N., Gopi, A.P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 35(3-4): 197-208. http://dx.doi.org/ts.34.197-208

[29] Gopi, P., Vejendla, L.N. (2017). Protected strength approach for image steganography. Traitement du Signal, 35(3-4): 175-181. http://dx.doi.org/10.3166/ts.34.175-181