ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (1016-1030), Month: April - June 2015, Available at: www.researchpublish.com

Improved Data Centers Privacy Using End-to-End Location Privacy on Cloud Environment

[1]Khushwant Virdi, [2]Anil Kumar

[1, 2] Department of Computer Science, Guru Nanak Dev University, Amritsar (Pb.), 143005, India

Abstract: **Cloud computing is a technology that provides the processing huge amount of data which depend on sharing computing resources like networks, servers, storage, applications, and services. The end-to-end location privacy has been neglecting in the field of cloud computing. Location privacy deals with the hide the location of source and high end server from the hackers by providing those fake locations so that hackers can utilize their maximum time to search the fake location instead of original location of source and destination or high end server. This dissertation has focus on various end-to-end location privacy techniques like forward random walk, bidirectional tree, dynamic bidirectional tree and zigzag bidirectional tree that can be applied in cloud computing. The paper has shown that the location privacy is required for cloud computing environment especially for public clouds network because user used to store his or her critical data on the cloud so cloud security is essential issue in the cloud computing.**

Keywords: **Cloud Computing, Location Privacy, Location Privacy Techniques and Algorithms, Types of Cloud.**

1. INTRODUCTION

Cloud Computing has been visualized as the next generation architecture of IT industries, due to its long roll of extraordinary advantages in the IT record: on demand self-service, universal network access, location self-determining resource pooling, quick resource stretch, usage-base charging and change of risk. As a disorderly technology with profound implication, Cloud Computing is transform that how business use information technology. One primary feature of this model is that data is being centralized or outsourced into the Cloud. From users point of view, including both individuals and IT industries, storing data distantly into the cloud in a flexible on-demand approach brings engaging benefits like relief of the stress for storing, managing, universal data access with self determining geographical locations and prevention of resources overheads on hardware, software, and personnel maintenances, etc. [1]. Cloud computing is a technology that provides the processing huge amount of data which depend on sharing computing resources like networks, servers, storage, applications, and services. cloud computing has emerged roughly in the year 2008 as a new distributed computing paradigm with the purpose of achieving the long dreamed computing as utility, a term first invoked as early as 1965 [2]. Few years ago, people used to store their files, documents, images on disks [3]. Then, more recently, most of the people move towards the memory sticks. Cloud computing refers to the capability to use and operate information stored on remote servers via any Internet-enabled service, including smart phones. Computing services and applications will gradually be distributed as a service, over the Internet network. For example Google Mail, Microsoft Office 3651 or Google Docs.

In the future, governments, industries and persons will rapidly turn to the cloud. The cloud computing model changes the technique in which information is managed, specially where individual data processing is concerned. End-users can use cloud services without any need for any professional perceptive of the fundamental technology. This is an important feature of cloud computing, which offers the benefits of sinking cost through the sharing of storage resources and computing resources , combined with an on demand provisioning model based on a pay-per-use business system. These novel attributes have an express IT funds and cost of ownership and membership, but also carry issues of fixed security, trust and privacy mechanism. Privacy in this section, refers to the accurate to self-government, that is, the right of persons to know? What is known about them?, be alert of store data about them, manage how that data is communicate and check its abuse. In other terms, it refers to more than just privacy of information. Protection of individual information derives from the right to privacy via the related right to self-determination. Every person has the right to control his own information, whether private, public or professional. Without awareness of the physical location of the server end-users consume cloud services without any information about the processes involved. Data store in the cloud can be easily manipulated and also easy to lose control of it. For instance, storing personal data on a server somewhere in cyberspace could create a major hazard to individual privacy. Cloud computing put numerous question related with of privacy and security like Are cloud servers reliable enough? Can cloud providers be trusted? What happens if data get lost? What about privacy and lock-in? Will switching to another cloud be difficult? etc. In these days location privacy is an important security issue because if the location of source and sink is not secure the hacker can easy track the location of traveling packet and can extract the critical information. Location privacy over a network is a challenging task.

Table 1: Difference Between Cloud Models [4]

Parameters	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Ownership	Third party	Organizati-on or Third party	Both	Both
Location	Off-Site	On-Site	Both	On-Site
Cost	Low	High	Medium	High
Security	Low	High	Medium	High
Scalability	Unlimited	Limited	Base plus burstable	-------------
Vmware Compartibil-ity	Yes	Yes	Yes	Yes
Talent	Multi Talent	Single Talent	Multi Talent	Multi Talent
Service level	Provider Specific	Internal IT Specific	Aggregate	------

2. LOCATION PRIVACY

Privacy concerns are gradually more important in the online world [3]. It is broadly acknowledged that cloud computing has the prospective to be privacy disable. The protected processing of individual information in the cloud represent a enormous challenge. Implementation of privacy-enhancing technologies to maintain such behavior in the cloud will depend upon the subsistence of regular ways of treating individual information at the global level and on technical principles which can assist to express compliance with permissible and authoritarian frameworks.

2.1 Source Location Privacy:

Source location privacy refers to the ability of protecting the location of the sender from where the data has been sent towards the high end server nodes.

Prior work in protecting location privacy to monitored objects wanted to increase safety period, which is defined as the number of messages initiated byte current source sensor before a monitored object is traced (Pavitha et al. (2014) [5]).

The source location privacy-preserving scheme can be distinguish into global adversary-based and routing-based schemes (P. Sengottuvelan (2013) [6]).

The global-adversary-based scheme assumes that the hacker can supervise each and every program in a communication link in the network. Every node has to send the information concurrently within the duration of time period. Routing-based schemes utilize weak presumptuous that the hacker has restricted overhearing capacity. The monitoring scheme starts from the sink and tries to establish the start of a transmission by backside tracing the hop-by-hop progress of the packets sent to the source node. Routing-based scheme seek to protect source nodes location privacy by transferring packets through different routes in place of one route, to make it infeasible for hackers to trace back info packets from the Sink to the source node because they cannot receive a continuous flow of info packets. However, if the hackers overhearing range is more than the sensor nodes transmission range, the probability of capturing a large ratio of the packets sent from a source node significantly increases. A hotspot is produced when a huge amount of packets are sent from the sensor nodes of a tiny region, causing an understandable inconsistency in the network traffic. A novel attack called Hotspot- Locating, where the hacker tries to make utilize the traffic changeability caused by hotspots to locate pandas by analyzing the data collected from the inspection points using traffic analysis techniques such as the nodes packet sending rates and packets correlation.

2.2 Destination Location Privacy:

Destination location privacy is generally committed to protecting the hacker from attaining the location of the base station (sink or high end server) . The base station (sink or high end server) is the most important part in the network because it immature for dealing out and analyzing all the information composed by the sensor nodes. Furthermore, it serves as an interface between the monitored fields and users, allowing the user to access or send guidelines to sensor nodes. Thus, hacker aware of the location of the base station can compromise it, or even demolish it, rendering the cloud useless (Pavitha et al. (2014) [2]). They also presented four different methods to protect the location privacy of destination from an eavesdropper. First, they proposed a multiple parents routing technique in which for every packet a sensor node choose one of its parents arbitrarily and pass the info_packet to that parent. This makes the traffic prototype between the source and the destination more isolated than the technique where every info_packets pass through the same series of nodes. After that they introduced scheme using controlled random walk, hot spots and random fake paths. The controlled random walk scheme add a random walk to the multiple parent routing technique cause the traffic prototype to be more extend out and hence less exposed to rate monitoring. The random fake path scheme was introduced to confuse hacker from tracing an info_packet as it moves towards the destination (sink, high end server). After that differential fractal propagation (DFP) scheme was introduce, whenever a node transmits a real info_packet, its fellow node generates a fake info_packet. This fake info_packet transmit configured number of hops to puzzle the hacker. They also planned a scheme for creating some region of high activity locally in the sensor network called hot spots. If such a region receives a info_packet, the info_packet has high chance of transmit through the same series of nodes creating an area of high activity. A local eavesdropper may be receiving into trust that this region is close to a destination (high end server). However, a global eavesdropper can observe that only some info packets generated by real things exceed through these hot-spots. The location privacy routing protocol (LPR) for destination location privacy [2] algorithm provide privacy to the destination (HES) with help of superfluous hops and fake Info_ packets when data is sent to the destination (HES). Every time an info packet is Figure 1: Forward Random walk forwarded to the next hop, the info packet may shift either nearer or far from the destination (HES). Along with the actual info packets, sensors may produce fake info_packets that go away from the destination to puzzle the hacker.

3. LOCATION PRIVACY SCHEMES AND ALGORITHMS

In this section different location privacy schemes and their algorithms has been discuss.

3.1 Forward Random Walk:

Hacker monitoring system as shown in Fig. 1, the source frequently sends info_packets to the HES by multi-hop communications network. If the info_packets are always delivered from source to HES along a same path, it will be simply for a hacker to recognize the location of both the source and HES via hop-by-hop tracking. Therefore, a solution to attain end-to-end location privacy is to change the delivery way, based forward random walk scheme (FRW). In this Scheme all nodes dispatch received packets to a node arbitrarily selected from its forward neighbors whose hop count to destination is not superior to its own hop count. The FRW scheme requires every node to acquire its hop count to the HES, which can be obtained by using a HES based-based flooding. At the starting, the HES will begin a flooding, after that every node can get together its own and its neighbor’s hop counts to the HES.

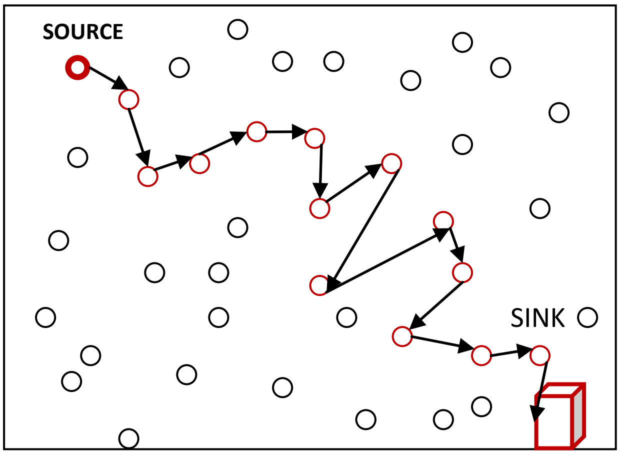

Figure 1: Forward Random walk

Here node i’s hop count to the high end server as Hi. Then it satisfies $|Hi - Hj| \leq 1$. If nodes i and j are the neighbor nodes. The neighbor place of node i is written as Ni. In the FRW scheme, each node i divides its neighbors into equivalent list, closer list and further list, which can be represented as ELi, CLi and FLi respectively. For every node in Ni with a hop count equal to Hi will be incorporated into ELi, for node i, every node in Ni with a hop count lesser than Hi will be incorporated into CLi and each node i Ni with a hop count superior than Hi will be included into FLi. The forward list of node i as the union of CLi and ELi, which is represented as FRLi. When a node detects the existence of the target, it will be a source node and sporadically send info_ packets to the HES. To forward the info_packet, a node will randomly select a neighbor from its forward list as the next hop.

Algorithm 1: Forward Random Walk

```
Initialize Next_hop = Null.
Build the forward list FRLi.
While Receive a message M do.
Randomly select neighbor from FRLi as Next_hop.
Forward the received info_packet to Next_hop.
end while
```

Consider that the next list will not be considered as the participant for the next hop since it will direct the info_packet further away from the HES, with a result of extremely increasing the latency. As a result, the info_packet will be travel through a FRW from source to HES. The method of the FRW scheme is illustrates in Algorithm 1.

3.2 Bidirectional Tree:

In the cloud computing, the hacker can threaten the location privacy of the source and HES by monitoring info_packets flow, a straight way to protect against these threats is to screen the source and HES in the tree topology created by the flow of transmitted info_packets, which makes difficult for the hacker to find them. Therefore, the tree topology in the BT scheme is employed to protect the end-to-end location privacy. Fig. 2 shows idea of the BT scheme.

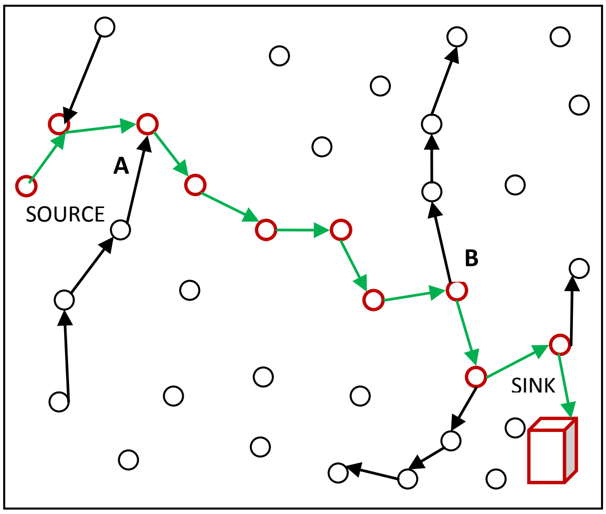

Figure 2: Bidirectional Tree

The original messages are transmitted through shortest route from source to HES. For the protection of source location privacy tree topology is designed along the shortest route at the source side, in which the fake messages are transmitted from the leaf nodes to the track nodes. As the hacker would try to trace the source by moving to the rear the direction of the info_ packets, the Branches of the tree will depart the hacker from the original delivery route, which can help to protect the source location privacy. Similarly, the tree topologies along the shortest route at the HES side are designed to protect the HES location privacy. The fake messages in the branches of tree are from the track nodes to the leaf nodes, which can misguide the hacker from the original delivery route to protect the HES location privacy since the hacker would track the HES by moving forward the direction of the info_packets.

Initially, the HES create a flooding such that every node can attain the hop count to the HES. Before sending monitoring packets to the HES, the source transmits a routing request message that includes its hop count Hs, to the HES along the shortest route. For each node i which receives the routing request message, $\mathrm{Hi} > \left(1 - \frac{\beta}{2}\right)\mathrm{Hs}$, it will arbitrarily choose a neighbor with probability Pn to produce a branch to defend the source location privacy, where β represents the percentage of nodes in the shortest route to produce the tree branches. Moreover, if $\left(\mathrm{Hi} < \frac{\beta}{2}\,\mathrm{Hs}\right)$, it will arbitrarily choose a neighbor with probability Pn to produce a branch to defend the HES location privacy. For example, assume ($\beta = \frac{2}{3}$), then a node i in the shortest route with ($\mathrm{Hi} > \frac{2}{3}\,\mathrm{Hs}$) will also originate a branch with probability Pn to protect the sink location privacy. A node i in the shortest route with ($\mathrm{Hi} < \frac{1}{3}\,\mathrm{Hs}$) will also create a branch with probability Pn to defend the HES location privacy. The nodes in between just relay the routing request message along the shortest path to the HES.

Algorithm 2 shows the process of the BT scheme. When node i receives an original message from a neighbor, it relays the message to a node in CLi. In addition, if $\mathrm{Hi} > \left(1 - \frac{\beta}{2}\right)\mathrm{Hs}$ node i produce a source side branch with probability Pn, where the length of the produced branch is L. Otherwise, if $\left(\mathrm{Hi} < \frac{\beta}{2}\,\mathrm{Hs}\right)$ node i generates a HES sides branch with probability Pn and length L. The generation procedures are described in Algorithms 3 and 4 respectively. The fake messages in the branches can digress the hacker away from the original delivery path. Thus, the BT technique can attain a long safety period against the eavesdropper. The parameters P and L also adjust to get a content performance. Let the source is Hs hops away from the high HES. As the original messages are sent along the shortest route, the latency will be Hs, indicating that the BT technique can send Figure 2. Bidirectional Tree the monitoring information to the HES with the minimum end-to-end latency. For the energy consumption, within TS, the average number of transmitted original messages in the network is Hs, and the average number of transmitted fake messages is βHsPL. Thus the energy consumption of the BT technique is:

$$(\mathrm{Hs} + \beta\mathrm{HsPL} = (1 + \beta\mathrm{PL}).\mathrm{Hs})$$

While BT technique can avert the eavesdropper from contravention the end-to-end location privacy, there is a potential risk if the eavesdropper can agree to a great strategy. The hacker may be receive, getting lost in the route between A and the source or the route between B and HES. However, a great hacker may be able to assume the route of the target based on its visited route V. If the hacker is looking for the source when it is near to B, as the original messages are sent along the shortest route, the hacker can track hop-by-hop from B to A. Then the hacker can assume that the source should be on the extending line of BA. Then, the hacker can travel directly along the direction of BA from A and with a high probability it can recognize the source as long as it gets close enough. The hacker can use the related policy to assume the direction of the HES as well.

Algorithm 2: Bidirectional tree

```
Initialize Next_hop = Null, Child_Node = Null
Build the Neighbor set Ni and the closer list CLi.
Random select a node from CLi as Next_hop.
Child_Node Random select(Ni - Next_hop).
While Receive a original message M do.
Forward the info_packet to Next_hop.
If  $\mathrm{Hi} > \left(1 - \frac{\beta}{2}\right)\mathrm{HS}$  then
Set TTL (branch_req, L).
Send branch_req to Child_node with probability P.
else if $\mathrm{Hi} < \left(\frac{\beta}{2}\right)\mathrm{Hs}$ then
Set TTL (Sink_dummy, L).
Send Sink_dummy to Child_node with probability P.
end if
end while
```

Algorithm 3: Source Side Branch Generation (Node i)

```
Initialize: Child_Node = Null,
Parent_node = Null.
while receive a branch_req message do
    Set parent_node as the sender of branch_req.
    TTL   Get TTL (branch_req).
    if TTL > 0 and Child_node = Null then
        Child_node   Random select (Ni)
        Set TTL (branch_req, TTL - 1).
        Forward branch_req to child_node.
    else if TTL=0 then
        Set TTL (source_dummy,L).
        Become a fake source and periodically
        send source_dummy to Parent_node.
    end if
end while
While receive a source_dummy message do
    TTL   Get TTL (source_dummy).
    if TTL > 0 then
        Set TTL (source_dummy, TTL - 1).
        Forward source_dummy to Parent_node.
    end if
end while
```

Algorithm 4: Sink Side Branch Generation (Node i)

```
Initialize: Child_Node = Null.
while receive a Sink_dummy message do
    TTL   Get TTL (sink_dummy).
    if TTL > 0 then
        if Child_node = Null then
            Child_node   Random Select (Ni)
        end if
        Set TTL (sink_dummy, TTL -1).
        Forward sink_dummy to Child_node.
    end if
end while
```

3.3 Dynamic Bidirectional Tree:

It's the combination of above both schemes i.e. FRW and BT scheme.

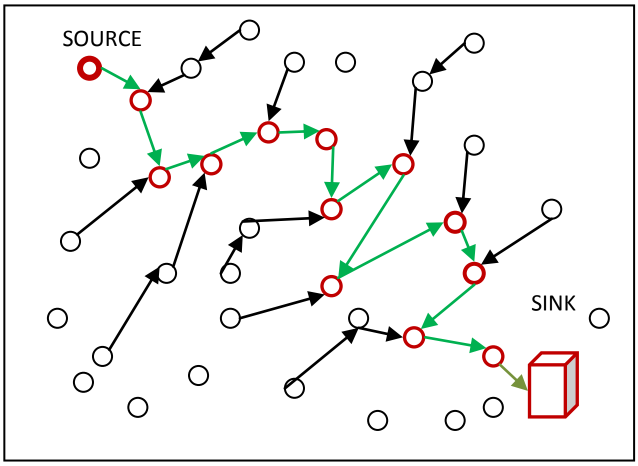

Figure 3: Dynamic Bidirectional Tree

To prevent the hacker from inferring the direction of the source or HES using the above method, the DBT scheme combines the FRW scheme and the BT scheme together. Fig. 3 illustrates the idea of In this the delivery route of the info_message differs as time passes i.e. the info_packet has traveling through geographical area from source to HES that may be easily increase the difficulties of hacker to trace the location of info_packets. To defend the origin location privacy a vibrant tree scheme can be used at the source side the DBT scheme. The release paths of the original info_message vary over time, which can increase the tracing difficulty for the hacker. Initially, the HES create a flooding such that every node can get its hop count to the HES. When the source sporadically sends monitoring info_packets to the HES, every node which receives the monitoring info_packet will arbitrarily select a neighbor from its forward list to forward the info_packet. Therefore, the original info_ messages will pass through a FRW from source HES. To protect the source location privacy, a dynamic tree topology will be adopted at the source side. Assume that the hop count of the source is Hs. When a node i receives an original message from its neighbor j, it will pass the real info_message to the next hop, which is arbitrarily selected from its FRLi. Also, if $\frac{\text{Hs}}{2} < Hi < Hj$, it will produce a source sides branch with probability P using a scheme similar to Algorithm 3. The major difference is that each fake source will only send fake info_message for D times. On the other hand, if Hi $< \frac{\text{Hs}}{2}$ and Hi $< Hj$, it will generate HES sides branch with probability P using a scheme similar to Algorithm 4. The major difference is that when a node receives a fake info_message, it will reselect a child node to relay this fake info_message, i.e., the branches at the HES side is dynamic. Algorithm 5 shows the procedure of the DBT scheme.

```
Algorithm 5: Dynamic Bidirectional Tree
Scheme (Node i)
Initialize: Next_hop = Null, Child_Node = Null.
Build the forward list FRLi.
while receive a real message m from node j do
Randomly select a node from FRLi as Next_hop and
forward the message to Next_hop.
Child_node   Random Select (Ni - Next_hop).
if Hs $< Hi < Hj$ then
Set TTL (branch_req, L).
Send branch_req to Child_node with probability P.
else if Hi $< Hs$ and $Hi < Hj$ then
Set TTL (Sink_dummy, L).
Send Sink_dummy to Child_node with probability P.
end if
end while
```

3.4 Zigzag Bidirectional Tree:

The zigzag bidirectional tree scheme (ZBT) is another end-to-end location privacy protection scheme used in cloud computing. It is used to prevent the hacker from finding the path of the source or HES. In the ZBT, the proxy source and the proxy HES is employed to make the real info_message are delivered along a zigzag path. As shown in Fig. 4, concentric circles A and B represent a proxy source and a proxy HES, respectively. In the pathway from the source to A, few topological branches will be produce to deviate the hacker away from the original delivery path of the real info_message to protect the source location privacy. In the next segment, the info_packets will be delivered along the minimum path length from A to B. In the path from B to the HES, some topological branches will also be produced to protect the HES location privacy. To assurance the efficiency of the ZBT scheme, several proxy HES ports are produce, which are deployed consistently around the HES. This is used to avoid a particular insecure situation that may or may not exist if only one proxy HES user is generated. In this situation, if the source unluckily plots very close to this proxy HES, then the performance of branches at the source side will not work effectively. Note that the number of proxy HES user should be suspiciously resolute. If a huge number of proxy HES users are produced, the proxy source will have more option to send the monitoring info_packets to the destination or HES, which is beneficial for the location privacy protection. Moreover every proxy HES node has to perform a flooding process for every node in the network to get the hop count which is more energy-consuming, high cost will be introduced if we use more proxy HES users. Thus an exchange should be made among the number of proxy HES nodes and the induced cost. As the zigzag routing will not work well if the proxy HES is closer to the source, the ZBT scheme will always choose the user which is auxiliary to the HES as the proxy HES. In the same way, when the monitoring info_packet is sent from the proxy HES to the HES, every node in the path will also produce a branch with probability P and length L. The monitoring info_message will be sent along the minimum pathway from the proxy source to the proxy HES without producing any branch. Algorithm 6 illustrates the working of ZBT scheme, and the branch produce procedures at the source and HES sides can be referred to Algorithms 3 and 4 respectively. Here Hp denote the hop count from the proxy source to proxy HES, then the end-to-end latency of the ZBT scheme is 2h + Hp, where h indicates the hop count from the proxy source to source and from the proxy HES to HES. For the energy consumption, the average number of transmitted original info_messages within interval TS is $2h + Hp$ and the average number of transmitted fake info_message is 2hPL. Thus, the energy consumption of the ZBT scheme is:

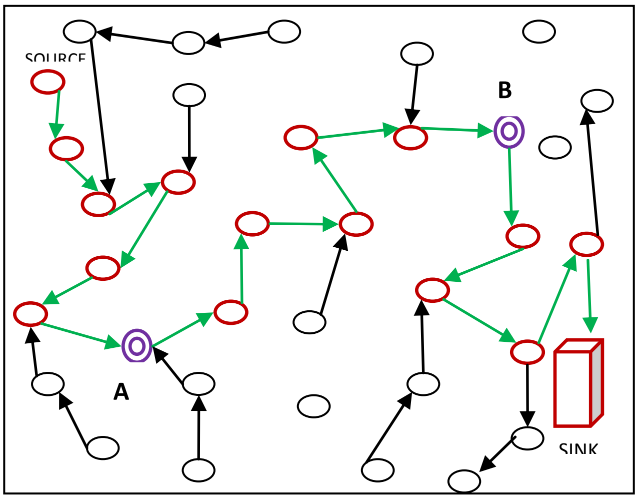

Figure 4: Zigzag Bidirectional Tree

$$2h + Hp + 2hPL = 2h(PL + 1) + Hp. (6)$$

Note that 2h + Hp $>$ Hs where Hs is the source node‘s hop count to the HES, which indicates that the energy consumption of the ZBT scheme is larger than Hs, i.e., $2h\ (PL + 1) + Hp > Hs$.

Algorithm 6: Zigzag Bidirectional Tree Scheme (Node i)

```
Initialize: Next_hop = Null.
while receive a real message m do
Destination   Get Destination (m).
if IsProxySource (Destination) = true then
if IsProxySource (i) = true then
Determine Next_hop and forward m towards proxy sink.
else
Determine Next_hop and forward m towards proxy source.
Child_node   Random select (Ni - Next_hop).
Set TTL (branch_req, L).
Send branch_req to Child_node with probability P.
end if
else if IsProxySink (Destination) = true then
if IsProxySink (i) = true then
Determine Next_hop and forward m towards sink.
```

```
else
Determine Next_hop and forward m towards proxy sink.
end if
else if Is Sink(Destination) = true then
if Is Sink(i) = false then
Determine Next_hop and forward m towards sink.
Child_node   Random select (Ni - Next_hop).
Set TTL (sink_dummy, L).
Send sink_dummy to Child_node with probability P.
end if
end if
end while
```

4. LITERATURE SURVEY

Recent expansion of cloud-based application and systems, a numerous technical organization have in progress to provide public storage cloud services, and upload user records or data in data centers located across the network. Whenever users used to store private data in common data centers, they drop control to store and access data. Several classes of personnel may or may not access the storage media. Whereas highly protected cryptographic techniques can protect user data. A new file system called BIFS (Bit-Interleaving File System) has been designed for highly protection of user data. Whenever user focuses on the on-disk state of privacy protection, BIFS re-arrange data in at the bit level, and then stores bit slices at distributed locations in the storage system (Sheng et al. (2011) [7]).

The cloud computing is updated as a novel computing technology where numerous services are available. In this technology location of data is maintained by a third party called service provider or vendor hence an individual person cannot manage their own data because of this reason, privacy on data is an essential concern for cloud computing both in terms of user trust and legal compliance. In cloud computing data privacy system are provided in which non-sensitive and sensitive data are maintained individually (Ray et al. (2011) [8]).

The task of providing on-demand service, elastic, cost effective and storage resources should be lies with the Cloud Service Providers (CSP). Infinite number of resource availability is only possible through virtualization technology and also through the availability of a shared pool of storage and computational resources. There are many issues raised on the aspects of security in the public cloud. Legal issues concern with physical location of data, security issues has been concerned with the safety of cloud against any kind of security attacks and other major issues concerns include like availability, data recovery and privacy (Surianarayanan et al. (2012) [9]).

A privacy-preserving scheme framework has been developed for participatory sensing contexts which rely on cryptographic technique and distributed computations in the cloud. Every person had represented, by a individual software agent, which had deployed on the popular commercial cloud computing services. The system enables individuals to analyses and aggregate sensor information by performing a shared distributed computation with multiple agents. Individual information has not disclosed to anyone, including the CSP. The distributed computation proceeds by having agents perform a cryptographic protocol which is based on a homo-morphic encryption scheme in order to aggregate information (Drosatos et al. (2012) [10]).

Since much enthusiasm for spatial database in distributed computing has been pulled in, studies on protecting area information security in distributed computing have been effectively done. Then again, since the current spatial change plans are feeble to vicinity assault, they can’t protect the privacy of clients who appreciate area based administrations from the distributed computing. Thus, a change plan for giving a safe administration to clients is needed. Another change plan taking into account a line symmetric change (LST). This plan performs both LST-based information dissemination and slip infusion change for averting nearness assault successfully (Yoon et al. (2013) [11]).

In cloud computing there are some issues related to privacy and security, like unauthorized access, data replication, loss of privacy, and regulatory destruction that require enough attention. The recent research enthusiasm for creating programming designing strategies to emotionally supportive networks in view of the cloud, the writing neglects to give a methodical and organized methodology that empowers programming architects to recognize security and protection necessities and select a suitable cloud administration supplier in light of such prerequisites. Here a novel system establishes that fills this crevice. Their structure fuses a displaying dialect and it gives an organized methodology that backings elicitation of security and protection prerequisites and the choice of a cloud supplier in view of the satisfiability of the administration supplier to the important security and protection necessities (Mouratidis et al. (2013) [12]).

In the growing structure of cloud computing, fulfillment of feasible levels of cloud clients' trust in utilizing cloud administrations is straightforwardly subject to viable relief of its related resultant security risk and impending risks. Among the different crucial security administrations needed to guarantee compelling cloud usefulness prompting improvement of client's trust in utilizing cloud offerings, those identified with the safeguarding of cloud clients' information protection are altogether essential and must be sufficiently developed to withstand the inevitable security risk, as stressed in this exploration paper. Here the likelihood of abusing the metadata put away in cloud's database so as to trade off the security of clients' information things put away utilizing a cloud supplier's straightforward stockpiling administration. It, then, proposes a structure taking into account database composition overhaul and element remaking of metadata for the safeguarding of cloud clients' information security. Utilizing the affectability parameterization guardian class participation of cloud database qualities, the database construction is altered utilizing cryptographic and also social protection safeguarding operations. In the meantime, unaltered access to database records is guaranteed for the cloud supplier utilizing element recreation of metadata for the rebuilding of unique database composition, when needed (Waqar et al. (2013) [13]).

Protection in the cloud is still a solid issue for the vast selection of cloud advances by undertakings which apprehension to really put their delicate information in the cloud. There is to be sure a need to have a proficient access control on the information put away and handled in the cloud foundation permitting to support the different business and nation based regulation requirements. In this point of view, a novel methodology of end-to-end protection arrangement authorization over the cloud foundation and in light of the sticky approach ideal model. In our methodology the information assurance is performed inside the cloud hubs and is totally straightforward for the applications. Researchers depict the idea and the proposed end-to-end building design and also an execution in view of the FUSE (File-system in User-space) innovation. This usage is executed on a situation of information get to and exchange control, and is additionally used to accomplish execution assessments. These assessments demonstrate that, with a sensible extra reckoning cost, this methodology offers an adaptable and straightforward approach to uphold different security imperatives inside the cloud base (B.Brezetz et al. (2013) [14]).

The expanding spread of Location based services (LBSs) has prompted a restored exploration enthusiasm for location based security, particularly location based access control. It additionally raises a concern on potential protection infringement because of the likelihood of distinguishing the client who demands a given administration taking into account his/her area data at the time of the appeal. To guarantee the believability and accessibility of LBSs, there is a squeezing prerequisite for tending to security and protection issues of LBSs in a synergistic manner. Here an imaginative access control instrument for LBSs has been proposed to empowering both fine-grained access control and viable security insurance. The proposed methodology is in view of the development of cryptographic spatiotransient predicates by method for effective secure number correlation (Zhu et al. (2013) [15]).

Blast technique to protect the base station from both packet tracing and traffic analysis attacks has been proposed. It provides privacy against the global attackers. The transmission range set of selected sensors is varied to confuse the attacker. For this, network is divided into two set of nodes called blast nodes and ordinary nodes. Receiver is present somewhere inside blast nodes. Blast node retransmits the packet sent by source node inside blast area which is then sent to the receiver. The adversary is not aware of communication between blast node and actual receiver. Hence, location privacy of the receiver is maintained (Chinnu et al. (2013) [16]).

A hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to the large packets originating from a small location has been defined. They also developed a realistic adversary model, assuming that the adversary can monitor the network traffic in multiple areas, rather than the entire network or only at single location. Using this model, they introduced a new attack called Hotspot-Locating where the hackers use traffic analysis techniques to locate hotspots. To reduce the energy cost, clouds are active only during data transmission and the intersection of clouds creates a larger merged cloud, to reduce the number of fake packets and also boost privacy preservation (Mahmoud et al. (2012) [17]).

Source-location privacy technique during routing to randomly select intermediate nodes before the info_message is delivered to the HES node has been proposed. They first explain routing through a solo randomly choose intermediary node away from the source node. Their investigation represent that this technique can provide best local source-location privacy. Whereas providing source-location privacy for WSNs, results demonstrates that the proposed method is efficient in energy consumption, having low transmission latency and high message delivery ratio. Simulation results demonstrate that the proposed schemes can achieve better performance in memorandum (information) delivery latency, energy consumption and memorandum delivery ratio (Yun Li et al. (2010) [18]).

A ring signature is used to verify the source node while protecting its spatial privacy. However another node must be preferred to prevent the possibility of a traffic analysis assail by hacker. A ring signature based authentication has been proposed to protect the privacy of a source node and make difficult to reach its target region. The ring signature provides privacy to the source, and the other users that are preferred from its neighborhood. The experiments also indicated that the scheme provided privacy and the performance penalty was negligible when optimal numbers of signers were used in the ring signature. With the increasing number of signers it requires larger memory size and communication overhead (Debnath et al. (2014) [19]).

The two techniques that helps prevent the leakage of location information are source simulation (SS) and periodic collection (PC). PC provides best location privacy, while SS provides trade-offs among message cost, privacy and latency. Through analysis and simulation results the proposed techniques shows best and helpful in protecting information location from the hackers. To formalized the location privacy issues under the model of a global eavesdropper and illustrate minimum average communication overhead needed for achieving a level of privacy. They also presented two techniques to provide privacy against a global eavesdropper. Analysis and simulation studies show that they can effectively and efficiently protect location privacy in sensor networks (K..Mehta et al. (2007) [20])

An efficient technique consisting of unspecified topology discovery and intelligent dummy info_ packet injection (IFPI) to defend the location privacy of base station Numerous topology discoveries eliminate the potential fear against base station within topology discovery period. Moreover, IFPI enhances privacy protection potency during data transmission period. Over given rules, comprehensive simulations shows that their scheme significantly improves privacy strength compared with offered strategies (Xinfeng Li et al. (2009) [21]).

A novel secure and energy aware routing (SEAR) protocol to address two issues concurrently through probabilistic random walking and balanced energy consumption SEAR is designed with two configurable parameters security level and energy balance control (EBC). EBC is used to implement energy balance and enlarge the lifetime. Level of security is considered to find the probabilistic division of the random walking that provides security in routing. The level of security can be illustrated by the info_message source on a message level. Theoretical analysis and OPNET simulation results demonstrate that the proposed SEAR can provide superb balance among energy consumption and routing efficiency while preventing routing trace back attacks (Di Tang et al. (2010) [22]).

In cloud computing primary concerning to protection and privacy obstruct a wide adoption by clients of enterprises. The main aim of cloud data security project is to plan cloud services adhering (CSA) to laws of government privacy. In particular, there are six-layers of security model and three level of security assurance for cloud computing. Finally researchers proposed Security Management as a Service (SMaaS) modules that enable clients to apply essential privacy and security operations which is based on the sensitivity of clients critical data (Doelizsches et al. (2010) [23]).

5. PROBLEM DEFINITION

The research work focus on providing the location privacy of both source and high end server by using zigzag bidirectional tree algorithm. Sometimes the user can deploy the critical information on the cloud by using storage as a service for this end-to-end privacy of source and high end server is very important to protect the critical information of users from hackers. Location privacy deals with the hide the location of source and high end server from the hackers by providing those fake locations so that hackers can utilize their maximum time to search the fake location instead of original location of source and destination.

This paper has focus on end-to-end location privacy of cloud user and high end servers. The review has shown that the location privacy has very significant research with respect to safety period but in cloud computing environment public network are used so safety become a critical issue. So to overcome this issue zigzag based location privacy algorithm has been introduced to secure the safety period and also energy consumption will be further remove by using the effect of data fusion.

6. OBJECTIVES

The objectives of this dissertation are described as following:

1. To propose end-to-end location privacy based cloud computing using zigzag bidirectional tree algorithm.

2. To reduce the energy consumption further data fusion will be used.

3. To draw the comparison between proposed and heuristic cloud computing based on the following parameters.

- Safe Path Hops
- End to End Latency
- Energy Consumption

7. PERFORMANCE ANALYSES

In this paper the experimental results are taken with the help of MATLAB 2013.

Table 2 shows the performance comparison of different three approaches as parameter name safe path hope analysis or safety period. It means that moment when hacker initiates the node tracing procedure i.e. snoop on the initial info_ packet and finish at the moment when hacker find or capture the high end server (HES). It is measures in terms of number of nodes visited. The visited nodes of different three approaches have been shown in table and comparison analysis is shown in fig 5.

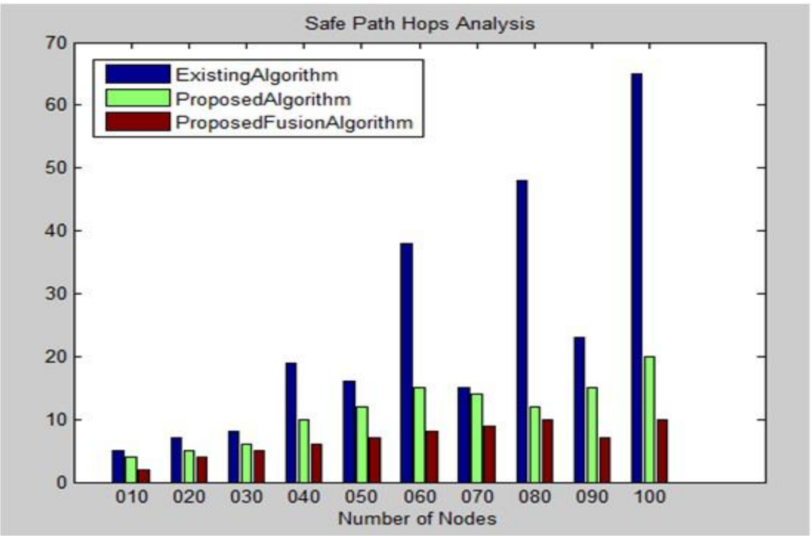

Figure 5: Safe Path Hops Analysis

Table 2: Safe path hops

Nodes	Existing Algorithm	Proposed Algorithm	Proposed Fusion Algorithm
10	5	4	2
20	7	5	4
30	8	6	5
40	22	10	6
50	24	10	4
60	41	15	8
70	15	14	9
80	16	12	10
90	22	15	7
100	75	20	10

Table 3 shows the performance comparison of different three approaches as parameter name energy consumption analysis. It means how much energy consumes to transmit the info_packet from source to HES. The results shows that the existing algorithm consumes more energy as compare to proposed algorithms i.e. new and fusion

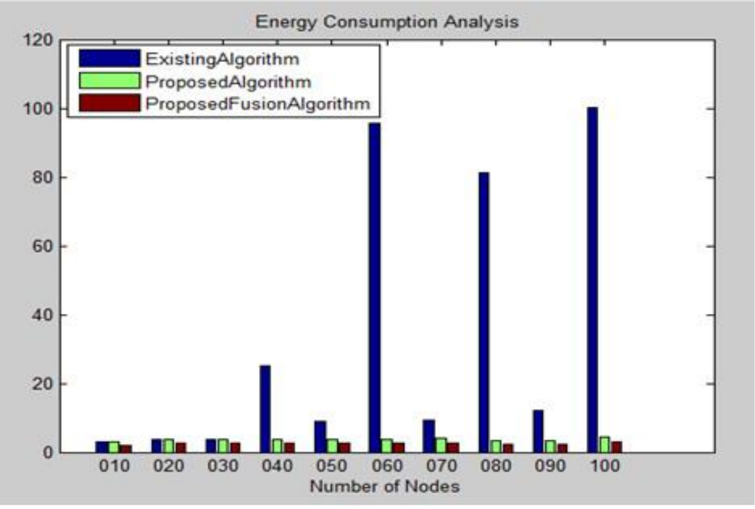

Figure 6: Energy Consumption Analysis

Fusion consumes less energy as compare to new because in fusion redundant (duplicate) data is removed or eliminated. The comparison analysis of different three approaches has been shown in fig 6.

Table 3: Energy Consumption

Nodes	Existing Algorithm	Proposed Algorithm	Proposed Fusion Algorithm
10	2.8765	2.3756	2.012
20	3.7686	3.3680	2.6386
30	3.5606	3.0609	2.4924
40	25.1106	3.7444	2.6177
50	8.1888	3.7396	2.6177
60	95.6899	3.5341	2.4739
70	9.2564	3.9707	2.7795
80	81.2047	3.1828	2.2280
90	11.9783	3.1855	2.2299
100	140.1762	4.2558	2.9791

Table 4 shows the performance comparison of different three approaches as parameter name end-to -end latency analysis. End-to-End latency means average time for an info_ packet to travel from initial point called source to sink i.e. HES. It is calculated in terms of info_packets average hop count from source to HES. The comparison analysis of different three approaches has been shown in fig 7.

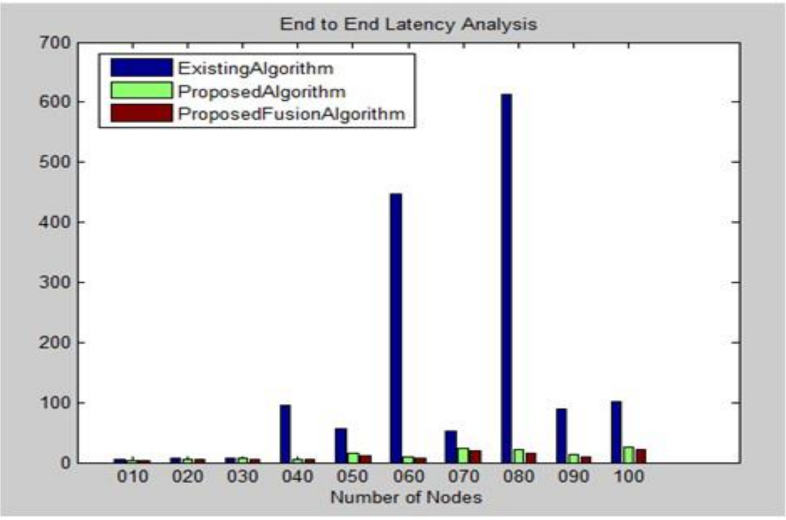

Figure 7: End-to-End Latency Analysis

Table 4: End-to-End latency

Nodes	Existing Algorithm	Proposed Algorithm	Proposed Fusion Algorithm
10	1.6056	1.5968	0.5919
20	5.9306	4.9658	3.8855
30	6.3455	4.3490	3.3671
40	95.5685	4.6569	1.6776
50	55.4934	15.5163	10.4685
60	447.5044	9.2218	7.2210
70	51.7781	23.9318	19.9671
80	712.0273	20.7987	15.7270
90	111.4260	13.9754	9.9582
100	120.3200	25.2522	21.2306

8. CONCLUSION

Cloud computing is a technology that provides the processing huge amount of data which depend on sharing computing resources like networks, servers, storage, applications, and services. The end-to-end location privacy has been neglecting in the field of cloud computing. Cloud provider provides the various services to the users. The user accesses the cloud services according to their needs. Sometimes the user can deploy the critical information on the cloud by using storage as a service for this end-to-end privacy of source and sink is very important to protect the critical information of users from hackers. Location privacy deals with the hide the location of source and sinks from the hackers by providing them fake locations so that hackers can utilize their maximum time to search the fake location instead of original location of source and destination.

This paper has focus on end-to-end location privacy of cloud user and high end servers. The review has shown that the location privacy has very significant research with respect to safety period but in cloud computing environment public network are used so safety become a critical issue. So to overcome this issue zigzag based location privacy algorithm has been introduced to secure the safety period and also energy consumption will be further removed by using the effect of data fusion. Due to the non availability of the actual environment, simulation environment is considered for the experimental purpose. The proposed technique is designed and implemented in the MATLAB 2013. The comparison has also been drawn among the proposed and the existing one based on the quality metrics of cloud computing environment. The comparison has clearly shown that the proposed technique outperforms over the available techniques.

9. FUTURE WORK

In the near future, this research work will be extending by increasing the nodes, range and some new parameters. This work has not considered the use of any swarm intelligence technique to enhance the results of the proposed technique further, so in near future we will use artificial bee colony (ABC) based technique to enhance the results further. Also some more quality metrics will also be considered.

REFERENCES

[1] Wang, Cong, Qian Wang, Kui Ren, and Wenjing Lou. "Privacy-preserving public auditing for data storage security in cloud computing." In INFOCOM, 2010 Proceedings IEEE, pp. 1-9. Ieee, 2010.

[2] Fernandes, Diogo AB, Liliana FB Soares, JoA£o V. Gomes, MÃ¡rio M. Freire, and Pedro RM InA¡cio. "Security issues in cloud environments: a survey." International Journal of Information Security 13, no. 2 (2014): 113-170.

[3] Goyal, Sumit. "Public vs Private vs Hybrid vs Community-Cloud Computing: A Critical Review." International Journal of Computer Network and Information Security (IJCNIS) 6, no. 3 (2014): 20.

[4] Guilloteau, S., and M. Venkatesen. "Privacy in Cloud Computing-ITU-T Technology Watch Report March 2012." (2013).

[5] Pavitha, N., and S. N. Shelke. "Providing Source and Sink Location Privacy against a Global Eavesdropper in Sensor Networks." International Journal of Research 1, no. 6 (2014): 63-68. 53

[6] Sengottuvelan, P. "Security Against Source Location Privacy Attack in Cloud Computing Using Keyword searching Technique."Research Journal of Computer Systems Engineering - RJCSE, June 2013.

[7] Sheng, Zhonghua, Zhiqiang Ma, Lin Gu, and Ang Li. "A privacy-protecting file system on public cloud storage." In Cloud and Service Computing (CSC), 2011 International Conference on, pp. 141-149. IEEE, 2011.

[8] Ray, Chhanda, and Uttam Ganguly. "An approach for data privacy in hybrid cloud environment." In Computer and Communication Technology (ICCCT), 2011 2nd International Conference on, pp. 316-320. IEEE, 2011.

[9] Surianarayanan, S., and T. Santhanam. "Security issues and control mechanisms in Cloud." In Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on, pp. 74-76. IEEE, 2012.

[10] Drosatos, George, Pavlos S. Efraimidis, Ioannis N. Athanasiadis, Ellie D'Hondt, and Matthias Stevens. "A privacy-preserving cloud computing system for creating participatory noise maps." In Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual, pp. 581-586. IEEE, 2012.

[11] Yoon, Min, Hyeong-Il Kim, Miyoung Jang, and Jae-Woo Chang. "Linear Function Based Transformation Scheme for Preserving Database Privacy in Cloud Computing." In Parallel and Distributed Systems (ICPADS), 2013 International Conference on, pp. 498-503. IEEE, 2013.

[12] Mouratidis, Haralambos, Shareeful Islam, Christos Kalloniatis, and Stefanos Gritzalis. "A framework to support selection of cloud providers based on security and privacy requirements." Journal of Systems and Software 86, no. 9 (2013): 2276-2293.

[13] Waqar, Adeela, Asad Raza, Haider Abbas, and Muhammad Khurram Khan. "A framework for preservation of cloud users? data privacy using dynamic reconstruction of metadata." Journal of Network and Computer Applications 36, no. 1 (2013): 235-248.

[14] Betgé-Brezetz, Stéphane, G-B. Kamga, M-P. Dupont, and Aoues Guesmi. "End-to-end privacy policy enforcement in cloud infrastructure." In Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on, pp. 25-32. IEEE, 2013. 54.

[15] Zhu, Yan, Changjun Hu, Di Ma, and Jin Li. "Cryptographic Spatio-temporal Predicates for Location-Based Services." In P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on, pp. 84-91. IEEE, 2013.

[16] Chinnu Mary George and Teslin Jacob, "Privacy Towards Base Station In Wireless Sensor Networks Against a Global Eavesdropper" A Survey, International Journal of Computer Science and Management Research, Vol 2, Issue, February 2013. pp. 1493-1497.

[17] Mahmoud, Mohamed MEA, and Xuemin Shen. "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks." Parallel and Distributed Systems, IEEE Transactions on 23, no. 10 (2012): 1805-1818.

[18] Li, Yun, and Jian Ren. "Source-location privacy through dynamic routing in wireless sensor networks." In INFOCOM, 2010 Proceedings IEEE, pp. 1-9. IEEE, 2010.

[19] Debnath, Ashmita, Pradheep kumar Singaravelu, and Shekhar Verma. "Privacy in wireless sensor networks using ring signature." Journal of King Saud University-Computer and Information Sciences (2014).

[20] Mehta, Kiran, Donggang Liu, and Matthew Wright. "Location privacy in sensor networks against a global eavesdropper." In Network Protocols, 2007. ICNP 2007. IEEE International Conference on, pp. 314-323. IEEE, 2007. 55.

[21] Li, Xinfeng, Xiaoyuan Wang, Nan Zheng, Zhiguo Wan, and Ming Gu. "Enhanced location privacy protection of base station in wireless sensor networks." In Mobile Ad-hoc and Sensor Networks, 2009. MSN'09. 5th International Conference on, pp. 457-464. IEEE, 2009.

[22] Tang, Di, Tingting Jiang, and Jian Ren. "Secure and energy aware routing (sear) in wireless sensor networks." In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, pp. 1-5. IEEE, 2010.

[23] Doelitzscher, Frank, Christoph Reich, and Anthony Sulistio. "Designing cloud services adhering to government privacy laws." In Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, pp. 930-935. IEEE, 2010.