Data Security using Trust by Integrating WSN and CC and Reputation Calculation Technique

Buddesab, Thriveni J, Venugopal K R

Abstract: ***Integration of Cloud Computing and Wireless Sensor Network led tremendous growth in the development of Information Technology, during the trust and reputation of service providers for information technology play an essential role. Cloud computing is web-based computing was in the services based on the internet such as data, storage, and computing resources are delivered to the local devices through the internet. Wireless sensor network deals with monitoring, gathering of the information about the physical or environmental conditions. The integration of these two domains has tremendous advantages to improve the business infrastructure and performance worldwide. The security of data on the cloud and calculation of trust and reputation of the Cloud Service Provides (CSP) and Sensor Network Providers (SNP) are the issues for this new paradigm. To fulfill these issues This paper presents novel techniques, for 1) trust and reputation calculation 2) data security on cloud 3) choosing desirable CSP and SNP for the service. This paper proposes Data Security by taking into account the services of Wireless Sensor Network (WSN) and Cloud Service Providers. Our experimental results help users to choose the best service providers in case of both Cloud and Wireless Sensor Network. In addition to that, data security is provided using a data encryption algorithm.***

Keywords: Cloud Computing, Data Security, Trust, Reputation, WSN, SNP and CSP.

I. INTRODUCTION

Wireless Sensor Network (WSN), is classified as one of developing innovations for the present source sequence time that has the control for alter the world. A WSN could be a group of sensors with a communications framework for observing and recording condition at distinctive locations. A network consists of multiple discovery locations called sensor nodes, each of the tiny, inconsequential and flexible [1]. Ordinarily observed limitations are weather determining, Traffic observing, crucial group capacities, home-based network, etc. A WSN system consolidates a access the provides wireless network back to the held together world and disseminated nodes. Potential solicitations of sensor systems incorporate: Industrialized computerization, Robotic and smooth households, Videotape observation, Traffic observing, Health scheme observing, Observing climate condition, Air traffic control and Robot control.

Revised Manuscript Received on October 05, 2019

Buddesab, Department of Computer Science and Engineering University Visvesvaraya College of Engineering Bengaluru - 560001, India
Thriveni J, Department of Computer Science and Engineering University Visvesvaraya College of Engineering Bengaluru - 560001, India
Venugopan K R, Department of Computer Science and Engineering University Visvesvaraya College of Engineering Bengaluru - 560001, India
Corresponding author: E.mail: tonnur21@gmail.com
Tel: +91-9945258825

Cloud computing is the distribution of computing administrations such as server, capacity, databases, network, computer program, analytics and more over the Web ("the cloud"). Or CC is for the conveyance of facilitated administrations over the web [3].Cloud computing facilitates the companies to utilize the compute asset, such as a capacity or an application, virtual machine (VMs), as a utility similar to power instead of having to construct and keep up computing foundations in house. Companies providing these computing administrations are called cloud service providers and regularly charge for cloud computing services based on utilization. Many of the things you'll be able do with the cloud: create modern apps and administrations, Store, back up and recoup information, Convey computer program on request, Host websites and blogs, etc.,[4],[5]. Cloud Computing is a considerably emerging innovation that gives on request computer program, equipment, infrastructure, and information capacity as administrations, in the meantime, WSN has more significant information collecting and observing capability. The combination of these two spaces is utilized around the world to progress the commerce Foundation and execution [6]. The combinations demonstrate has shown in Fig.1. Essential information is collected from the sensor network through different sensor nodes conveyed in multiple physical areas. The composed information is ordered, and protected information is encouraged into the Cloud platform. At last, Clients can get to the administrations of CSP complete the web.

Cloud security is the method of safeguarding life-threatening data from robbery, information outpouring, and alteration. A cloud platform offers many confidence services to address multiple necessities required to the information security. Distributed Security can be designed utilizing distinctive innovations and strategies such as utilizing

1. Strict Regulatory Standards.
2. Security Tools.
3. Distributed Denial of Service (DDoS) Mitigation.

Security falls into two classifications: security problems challenged inevitably with cloud providers additionally security problems looked toward their customers. A few security problems are associated with cloud data service: not just all inclusive security hazards, for instance, listening in, unlawful intrusion, forswearing of administration assaults, organization assaults, yet additionally specific Distributed computing hazards, for cases, side-channel assaults, and sick usage regarding cloud service. There is numerous approaches to give data security. The most well-known and generally utilized method is "encryption." Data encryption is the way

toward changing over data into a mixed up structure utilizing explicit calculations.

A. Motivation

During the combination of WSN and CC, the critic issue that should be well thought-out is the security of the information in cloud. As the security of the information is more fundamental for each area (navy, commercial...) it must establish in such a way that CSU won't develop undermined information.

B. Research Contribution

The important contribution of this paper is

1. This paper investigates the security of the information within the cloud for the CC-WSN integration and calculates the trust and reputation of CSP and SNP..
2. This paper proposes an calculation for the security of the information put away within the cloud. It too verifies CSP and SNP, and after that calculates trust and reputation of the administrations of CSP and SNP, to empower CSU to select true and alluring CSP and helps CSP in selecting honest to goodness suitable SNP..
3. It investigations the feedback of each user and keeps in track of the malicious feedbacks given by clients to honest to goodness providers.

C. Organization of this paper

Section II Presents related work, and Section III discussed the System Architecture and its description. The algorithms and schemes for the security of the cloud is proposed in Section IV. Performance Evaluation Trust and Reputation in Section V. Finally, this paper is concluded in Section VI

II. RELATED WORK

Zhao *et al*.,[7] have proposed a smart security framework dependent on WSN is proposed to solve the issue such a severe load utilization and testing to extend. The receives half and half topology structure dependent on cluster and altered cluster head choice calculation. Subsequently, this causes a decrease in energy cost in the arrangement period of sensor hubs when contrasted and LEACH calculation. The utilizing of the installed framework improves the strength of remote information transmissions.

Han *et al*.,[8] have proposed the trust-based protection instrument for WSNs are considered. Three sorts of trust data are considered, for example, Trust the executives to the robust geographical directing, Reputation-based confidence the board, and Group-based confidence the board conspire. In the wake of breaking down the security issue and trust the board for WSNs, an examination investigation of two trust the board models are taken with vitality protection and delayed system lifetime.

Zhu *et al*.,[9] have proposed a context non-mindfulness issue between flexible client and WSNs, which impacts the portable client getting the appealing data when planning WSNs and MCC is considered. The system performs data recommendation, data figure, just as data activity watching within the Cloud to induce the data incorporate information required by the flexible clients and potential status of WSNs. For giving attractive information, and forecast APRIORI calculation and the auxiliary exponential smoothing model (SESM) calculations are utilized separately.

Takabe *et al*.,[10] have proposed the a worldwide temperature alteration expanded by IT is considered, and Green IT is perceived as one of the answers for a dangerous atmospheric deviation. BEMS and HEMS are viable vitality sparing plans dependent on the representation, control, and the executives of vitality devoured by IT hardware. Sensor organize innovation is generally utilized in such frameworks. In ordinary HEMS, a costly hub is required to imagine the aftereffects of dissecting vitality utilization. Sews depends on the use of a cloud and a sensor organize.

Sun *et al*.,[11] have projected the framework for trust assessment in dispersed systems. The Trust assessment framework is utilized in specially appointed systems for verifying impromptu steering and helping malicious node identification. The benefit of the trust assessment framework improve arrange throughput just as assistance noxious hub recognition. Reproductions are likewise performed to explore different malevolent assaults.

Rehman *et al*,.[12] have suggested the fundamental issue in WSN is its limited assets. It looks the assets to sort Message Authentication Code (MAC) remembering the achievability of the procedure utilizedr the sensors arrange within reach. This paper researches distinctive cryptographic systems, for example, symmetric-key cryptography and asymmetric key cryptography.

Garg *et al*.,[13] have discussed about the creating intrigued for Cloud establishment has drastically extended the essentialness utilization of server ranches, which has turned into a fundamental issue. The high essentialness utilization not just implies high operational taken a toll, which reduces the net income of Cloud providers however in expansion prompts tall carbon surges which are not normally welcoming. Along these lines, essentialness beneficial courses of action are required to constrain the impact of Cloud handling on the soil. The Deep examination of Cloud is required concerning their capacity capability. The distinctive components of Clouds which include to the all out essentialness utilization and furthermore the consequences of these answers for future investigate orientation to enable green Cloud Computing is inspected. This also clarifies the work of Cloud clients in finishing this objective.

Das *et al*.,[14] have proposed the qualities of multi-agent frameworks present vulnerabilities and dangers for giving verified correspondence. One practical approach to limit the dangers for assess the trust and reputation for interfacing agent. Numerous trust and reputations models have through as such; however they neglect to appropriately assess trust when noxious specialists begin to act in an unusual manner. In addition, these models are incapable in giving a fast reaction to a vindictive operator's swaying conduct. Another part of multi-agent frameworks which is getting to be basic for supporting great administration quality is the even dissemination of remaining burden among administration giving agent.

Pujol *et al*.,[15] have discussed the issue of manipulative a level of reputation for operators going about as partners to the individuals from an electronic network is discussed about solution.

The Usual reputations systems depend on input after communication between operators. An elective method to set up reputation is identified with the situation of every individual from a network inside the comparing social community. The strategy depends on this thought, which is additionally utilized by understood positioning calculations, its properties just as test results and looks at them to other reputation systems for electronic networks supported by operator

Ganerwal *et al*.,[16] have proposed the conventional methodology of giving system security has been to get apparatuses from cryptography and verification. The traditional perspective on security dependent proceeding cryptography unaided is not adequate to exceptional attributes and novel mischievous activities experienced in sensor systems. A reputation-based system for sensor systems wherever hubs keep up a reputation for different hubs and use it to assess their dependability is proposed. This framework gives a versatile, different, and a comprehensive methodology for countering a wide range of mischievousness coming about because of pernicious and broken hubs. The framework utilizes a Bayesian plan, explicitly a reputation framework, for reputation portrayal, updates, and combination.

Josep *et al*.,[17] have presented the Usual reputation systems depend on input after communication between managers. An elective method to build up reputation is identified with the situation of every individual from a network inside the relating social community. The technique depends on this thought, which is additionally utilized by understood positioning calculations, talk about its properties just as test results and contrast them with other reputation instruments for electronic networks upheld by managers. The utilizations just neighborhood data so as to separate reputation, and it can adjust naturally to the topology of the system.

Li *et al*.,[18] have proposed the keeping up information security and proficiency of data preparing in cloud-WSN are imperative and exciting issues. The well-organized information contract out scheme based on CP-ABE, it can guarantee not as it were protected information access then moreover diminish by and large information handling time is displayed. The huge record is separated into a few information pieces by Information Owner (IO) at that point, the information pieces are encrypted and transmitted for the cloud server in comparable. For Information Recipient (IR), information decoding and information transmission are moreover prepared in parallel. The execution assessment shows that this scheme can significantly make strides information preparing proficiency compared to the conventional strategies

Ruj *et al*., [19] have proposed the decentralized get to control scheme for secure data storage in the clouds, that underpins mysterious confirmation. The Cloud confirms the authenticity of the user with-out knowing client's identity some time recently putting away information. Too provides get to control in which as it were substantial clients are able to decode the stored data. The scheme anticipates replay attacks and fortifies formation, adjustment, and checking data consume within Cloud. Key dissemination is exhausted a decentralized way.

Fortino *et al*.,[20] have proposed the framework gives a stage to construct and direct solicitations based on body sensor systems. The sensor hubs sent interior the body can be utilized to screen frameworks and people conditions in a wide run of application spaces. The integrates perceptions such as adaptableness and adaptability of assets, sensor heterogeneity, and the energetic arrangement then administration of client and public application

III. SYSTEM ARCHITECTURE

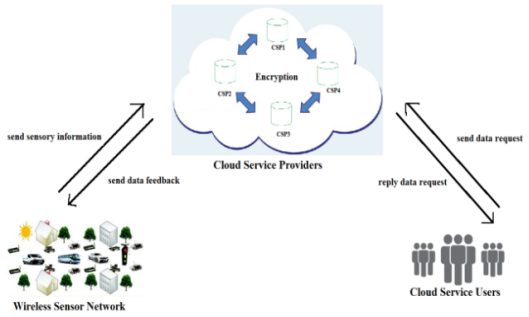

Fig.1. Combination of secure CC with WSN

Fig.1. Shows the framework design for the combination of two developing and dominant areas, for example, WSN and CC. The symbolizations utilized are given in Table 1. The combination of these two areas has increased a great deal of consideration from both engineering and academic world [21]. Information safety and certified response assurance for each client is the most significant thing that should be well thought-out and actualized. As information steeling and information alteration by the outsider before received at the legitimate clients has expanded. Appropriate information security should be accommodated the information in the cloud.

Table 1. Symbolizations utilized

Symbols	Definitions
CC	Cloud Computing
WSN	Wireless Sensor Network
CSP	Cloud Service Provider
SNP	Sensor Network Provider
CSU	Cloud Service User
Tcu	Trust unit of service from CSP to CSU
Tku	Trust unit of service from SNP to CSP
Rc	Reputation unit of service given by CSP
Rk	Reputation unit of service given by SNP
Tscu	Minimum trust unit of service from CSP to CSU
Tskc	Minimum trust unit of service from SNP to CSP
ct_c	Certificate of CSP
ct_k	Certificate of SNP
CSC	Cloud Service Charge

A. Overall Description of System Architecture

Recognize cloud C, and there will be a number of CSPs such as CSP_1, CSP_2, CSP_3, ...CSP_n and Similarly WSN well-known as WSN_1, WSN_2, WSN_3,.....WSN_n. The conveyed sensors collect the tangible information such as

activity, video, mugginess, temperature, weather, and sent to the different clouds. Here WSN acts as an data source, i.e., WSN gives essential information to CSPs. The CSPs acts as information collectors, organizers, and benefit suppliers to cloud benefit clients. At last, the clients i.e. CSU1, CSU2,.....CSUn is the information requesters for the CSP and CSPs are information requesters for SNP.

B. Factors of Trust and Reputation Calculation of CSP

Trust calculation is based on a few components based on how the information is given, how information is gotten to, whether there's a repetition of information etc. CSP gives the desired information to the clients on request. Based on the conveyed information and security given to the clients for their get to, CSU chooses the benefit of specific CSP.

1. Cloud Data Processing Unit

This relates whether cloud forms the crude tangible information with the mistake or without mistake. The non-mistake number (Sc1) and mistake number (Fc1) of information for each benefit from CSP to CSU. The information preparing unit (Tc1) is calculated utilizing condition (1)

$$T_{c1} = \frac{S_{c1}+1}{F_{c1}+S_{c1}+2} \qquad (1)$$

2. Cloud Data protection Unit

This trust compares to the tangible information put away on the cloud that can be gotten to by others or not-this esteem calculated based on the feedbacks around the past transmission on each benefit to specific CSU. The number of tangible information gotten to by others with regard to specific benefit from CSP to CSU is Fc2. The trust esteem of information protection unit (Tc2) is given by condition (2)

$$T_{c2} = \begin{cases} 1, & F_{c2} = 0 \\ 0, & F_{c2} > 0 \end{cases} \qquad (2)$$

3. Cloud Data Transmission unit

This trust with regard to whether the information is transmitted effectively to CSU or not. They are utilizing the feedbacks from CSU with respect to past exchanges with CSP the victory number (Sc3) and disappointment numbers (Fc3) are considered. The cloud information transmission unit (Tc3) is given by condition (3).

$$T_{c3} = \frac{S_{c3}+1}{F_{c3}+S_{c3}+2} \qquad (3)$$

The trust unit Tcu of each benefit from CSP to CSU is calculated with combination function (i.e. CF) of the over three believe units utilizing condition (4)

$$T_{cu} = \frac{(T_{c1}+T_{c2}+T_{c3})}{3} \qquad (4)$$

4. Reputation Service of CSP

The numeral of CSUs the select benefit of the CSP is CNc, and the numeral of CSUst the needs benefit for get from specific CSP is N'u. At that point the reputation unit (Rc) is considered utilizing condition (5).

$$R_c = \frac{CN_c}{N'_u} \qquad (5)$$

C. Factors of Trust and Reputation Calculation of SNP

1. Sensor Data Collection Unit:

This refers to whether the SNP collects the specified information with the mistake or without mistake. The non-mistake number and mistake number of information collection for each benefit from SNP to CSP are Sk1 and Fk1, separately. The believe unit of sensor information collection unit (Tk1) is calculated utilizing condition (6).

$$T_{k1} = \frac{S_{k1}+1}{F_{k1}+S_{k1}+2} \qquad (6)$$

2. Sensor Network Lifetime Unit:

This trust tells almost whether the lifetime of the conveyed sensor matches the real-time sensor or not. The coordinating number and non-matching number of the sensor arrange lifetime of each benefit from SNP to CSP are Sk2 and Fk2 individually, with the feedbacks on each benefit from SNP to CSP. The sensor network lifetime unit (Tk2) is calculated utilizing condition (7).

$$T_{k2} = \frac{S_{k2}+1}{F_{k2}+S_{k2}+2} \qquad (7)$$

3. Sensor Network Response Time Unit:

This trust tells whether the reaction time of the genuine conveyed sensor organize matches the sensor organize reaction time the SNP conveyed. The reaction time of the sensor organize is very an vulnerability due to different variables (e.g., sensor kicks the bucket, terrible climate). The coordinating number (i.e., Sk3) and non-matching number (i.e., Fk2) of the sensor arrange reaction time of each benefit from SNP to CSP. The sensor arrange reaction time unit (i.e., Tk3) is calculated by condition (8)

$$T_{k3} = \frac{S_{k3}+1}{F_{k3}+S_{k3}+2} \qquad (8)$$

4. Sensor Data Transmission Unit

This trust says whether the information transmission from SNP to CSP is successful or not. The victory number (i.e., Sk4) and disappointment number (i.e., Fk4) of information transmission of each benefit from SNP to the CSP based on the feedbacks of the past communication are considered for this calculation. The sensor information transmission unit (i.e., Tk4) is calculated by condition (9)

$$T_{k4} = \frac{S_{k4}+1}{F_{k4}+S_{k4}+2} \qquad (9)$$

Assuming that these four types of trust units, the combination function (CF) of these four trust values is taken as the trust unit Tkc of the benefit from SNP to CSP. This is often calculated utilizing condition (10).

$$T_{kc} = \frac{(T_{k1}+T_{k2}+T_{k3}+T_{k4})}{4} \qquad (10)$$

5. The reputation of Service of SNP

By considering the feedbacks of past transmission approximately the benefit, in the event that the CSP select the benefit of an SNP, implies that the CSP trusted the SNP and chosen to induce benefit from SNP.

The number of CSPs that chose the benefit of the SNP is CNk, and the number of CSPs that needs the benefit to get from an SNP is N'c. The notoriety unit RK of the benefit of the SNP is calculated utilizing condition (11).

$$R_k = \frac{CN_k}{N'_c} \qquad (11)$$

IV. PROPOSED SCHEMS

1. Passage list

For all CSPs and SNPs i.e. CSP = {CSP1, CSP2 CSP…….....CSPn} andSNP={SNP1,SNP2,…….....SNPn} who registers to the system with different parameters comes beneath Passage List. The Passage List of CSP is taken as P1, and Passage List of SNP is taken as P2.

2. Trust List

For all CSPs and SNPs i.e. CSP = {CSP1, CSP2,.....CSPn} and SNP={SNP1, SNP2, ...SNPn} with whom the CSUs or the CSPs concurs to induce the benefit based on the past believe and reputation values come beneath Trust List. The Trust List of CSP is taken as T1, and Trust List of SNP is taken as T2.

V. ALGORITHMS

A. Algorithm for Choosing desired CSPs for the service

Step 1: CSU reads Passage list (P1) and Trust list (T1).
Step 2: Checks *Tcu* and *Rc* values ∀ CSP ∈ Trust list.
Step 3: Compare *Tcu* and *Rc* values with *Tscu* and *Rsc* respectively.
Step 4: If *Tcu* ≥ *Tscu* and *Rc* ≥ *Rsc*
Step 5: Choose CSP for the service.
Step 6: Finish

CSU checks for the passage list and trust list. The trust list incorporates the passages of CSP who's Trust, and Reputation values are more than or rise to to the standard esteem of Trust and Reputation. The passage of CSPs, who is prepared to supply benefit to the client comes beneath the passage list. CSU issues ask to the server and get the Tcu and Rc esteem for each benefit from CSP to the CSU. CSU checks in the event that the Tcu and Rc esteem is more than or rise to to the Tscu and Rsc esteem and channel out the CSPs that are not fulfilled. CSU chooses the benefit of CSP on the off chance that it fulfills all the condition of CSU else select another CSP for the benefit.

B. Algorithm for Choosing desired SNPs for the service

Step 1: CSP reads Entry list (E2) and Trust list (T2).
Step 2: Checks *Tkc* and *Rk* values ∀ SNP ∈ Trust list.
Step 3: Compare *Tkc* and *Rk* values with *Tskc* and *Rsk* respectively.
Step 4: If *Tkc*≥ *Tskc* and *Rk* ≥ *Rsk*
Step 5: Choose SNP for the service.
Step 6: Finish

CSP checks for the passage list and trust list. The trust list passages incorporate the SNP who's Believe, and Notoriety values are more than or break even with to the standard esteem of Trust and Reputation. The section of CSPs who is prepared to supply benefit to CSP comes beneath the section list. CSP issues ask to the server and get the esteem Tkc and Rk for each benefit from SNP to the CSP. CSP checks on the off chance that the Tkc and Rk esteem is more than or break even with to Tskc and Rsk esteem and channel out CSPs that are not fulfilled. CSP chooses the benefit of SNP in the event that it fulfills all the condition of CSP else select another SNP for the benefit.

C. Algorithm for Securing Data within the Cloud

Input: Reads the file from WSN
Output: outputs encrypted file to CSU
Step 1: CSP reads the input file from the WSN and process using CRYPTO.
Step 2: CRYPTO (input file, key, output file)

```
{
  ∀ CSPi∈ (CSP && Trust list)
        Gets (input file) from WSN
                Encrypt (input file, key)
                Store (output file)
}
```

Step 3: Access the user requests
Step 5: Authenticate

```
∀ CSPn ∈ CSU
  if(Name && Password= valid)
    Valid users;
  Else
    Reject access;
```

Step 6: CSP accept the request of valid users.
Step 7: process the request.
Step 8: send the requested file in encrypted.

At first, the data accumulated from the sensor network is taken as input. The information is collected from the sensor nodes sent in a specific region. The collected data from the sensor arrange is scrambled by utilizing "CRYPTO" and organized into different suppliers. The substantial clients can get to the secured data put away on the cloud. After getting to the information on the cloud, clients get the scrambled record on the cloud. The clients can unscramble the desired data of their choice.

VI. PERFORMANCE EVALUATION

A. Preliminaries

The proposed system has 2 phases

1. Trust and reputation Calculation
2. Analyzing the feedback of the users to get genuine trust and reputation [22].

B. Simulation Setup

The sensor system is set up where the natural circumstance should be observed. The conveyed sensor accumulates the information, and afterward this information is sent to the Service Providers. The CSPs at that point compose the data as per the particular fields. The clients can approach the put away secure information in the cover over the web. The hard disk 40GB and RAM is set to 35 GB. The Operating System is Windows 8.1/XP is utilized with the JAVA/J2EE language. The coordinated improvement condition is Net Beans 6.9.1 with MYSQL database.

C. Performance Analysis

The analysis of trust and reputation of together cloud and WSN is measured. The numerous factors of cloud trust values are well thought-out and associated with the existing system values.

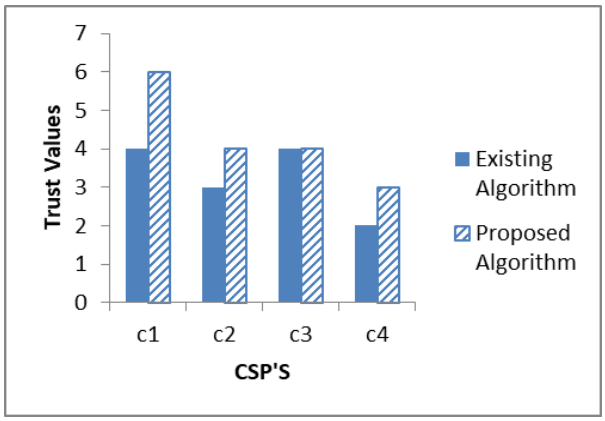

Fig.2. Cloud Data Processing Trust values Vs various CSP's

Fig.2.Shows Cloud Data Processing Trust values of various CSP's. As compared to c2, c3, c4, c1 has higher trust since it processes the raw sensory data without error. Hence c1 is a desirable choice by the users.

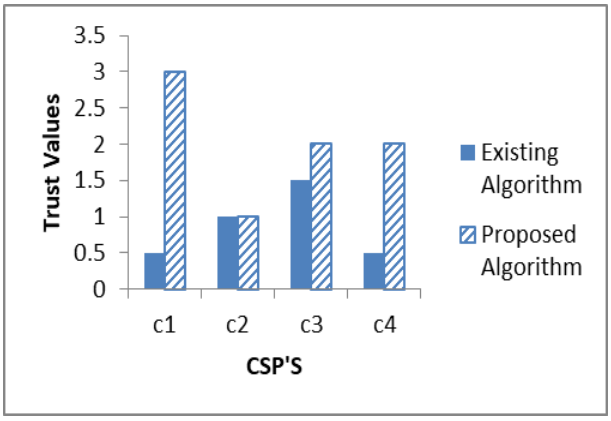

Fig.3. Cloud Data Privacy Trust values Vs various CSP's

Fig.3.Shows Cloud Data Privacy Trust values of various CSP's of cloud service providers. Here c1 has a higher value as compared to other providers since c1 provides better security to the user's data. Hence c1 is the desirable choice by users for accessing the service.

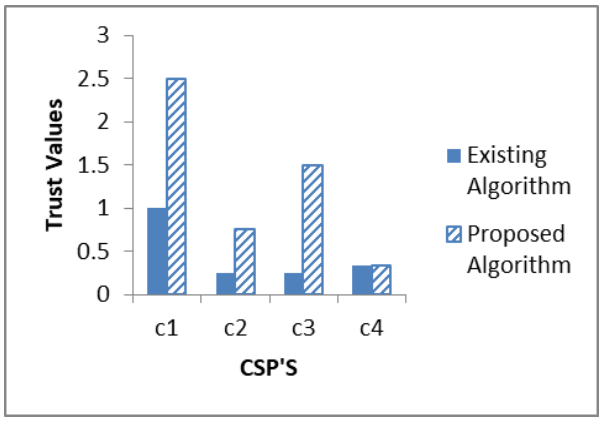

Fig.4. Cloud Data Transmission Trust values Vs various CSP's

Fig.4. Shows Cloud Data Transmission Trust values of various CSP's which reveals whether the data transmission between the information providers and data users is successful. As compared other providers, c1 and c3 have higher trust value since the data transmission between providers and users are almost successful. Hence c1and c3 is the desirable choice by users for accessing the service

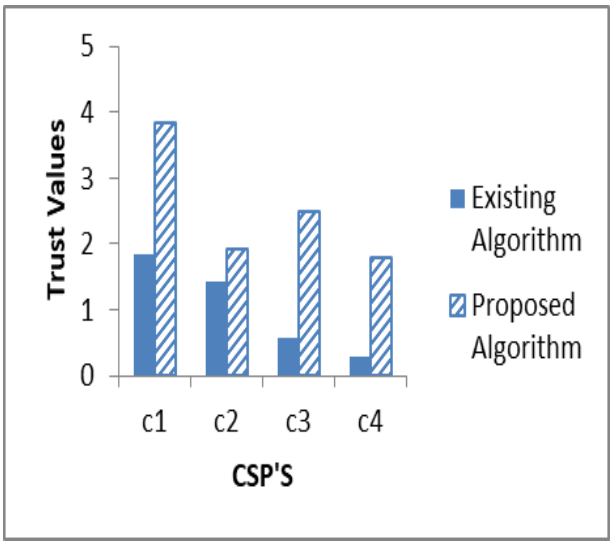

Fig.5. Comparison of trust values Vs various CSP's

Fig.5. shows trust values of various CSP's is more for the proposed method as compared to the existing as in the proposed method. Feedback of the CSU's is used to calculate the trust value, and Feedback analysis is done to remove false feedback and thus increase the trust value of the genuine service providers as compared to others c1 has higher trust values by considering all cloud trust factor values. Hence c1 will be the desirable choice for accessing the service by its users.

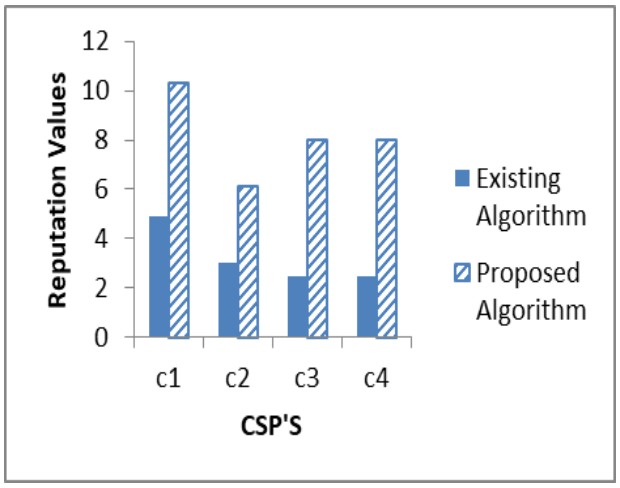

Fig.6. Reputation Values Vs various CSP's

Fig.6. shows the Reputation values of different CSP's is more for the proposed method as compared to the existing as within the proposed strategy. Feedback of the CSU's is utilized to calculate the Reputation esteem, and Feedback investigation is done to evacuate wrong criticism and in this way increment the reputation esteem of the honest to goodness service providers. As compared to others, c1 has higher reputation values by considering all cloud believe calculate values. Subsequently c1 will be the alluring choice for getting to the benefit by its clients.

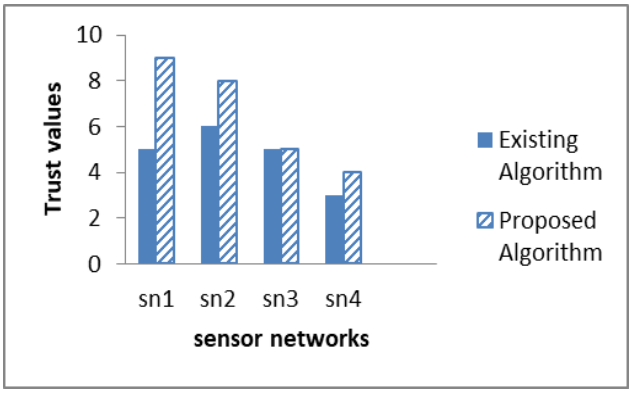

Fig.7 Sensor Data Collection Trust values Vs various SNP's

Fig.7. shows Sensor Data Collection Trust values of various SNP's data collected by the SNP's are true the situation. Based on the usage of the data on CSP's. SN1 has higher trust values compared to other SNP.

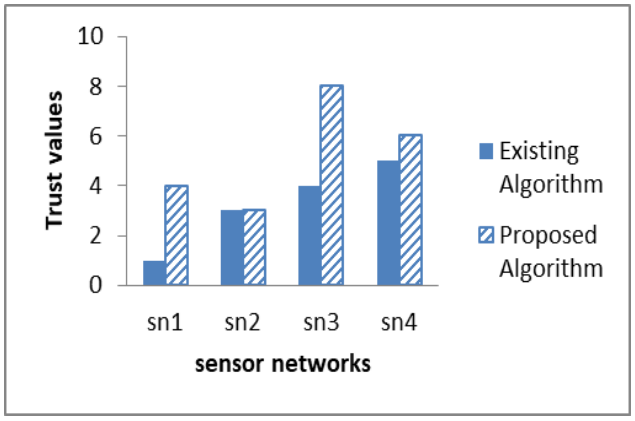

Fig.8. Sensor Network lifetime Trust values Vs various SNP's

Fig.8. shows Sensor Network lifetime trust values of various SNP's compares the network lifetime of the existing values SNP's to that of Proposed Values of SNP's. By using feedback analysis algorithm, the validity of the SNP's will increase hence led to increasing of network lifetime of SNP's. Here SN3 has more trust value compared others SNP's hence it is a desirable choice.

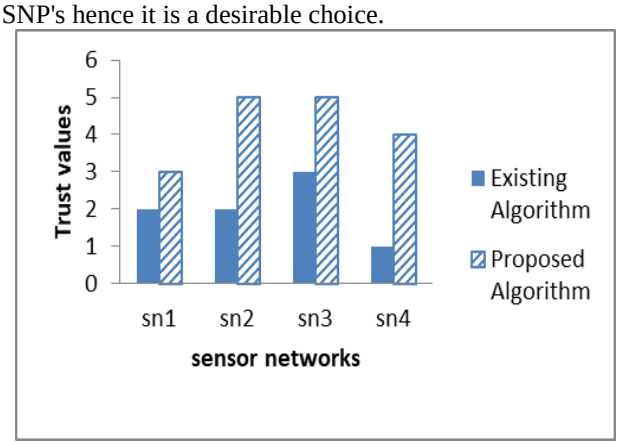

Fig.9. Sensor Network Response Time Trust values Vs various SNP's

Fig.9 shows Sensor Network Response time trust values of various SNP's how the SNP's will respond to the particular request of CSP's in the required time. Here SN2 has higher values compared to others.

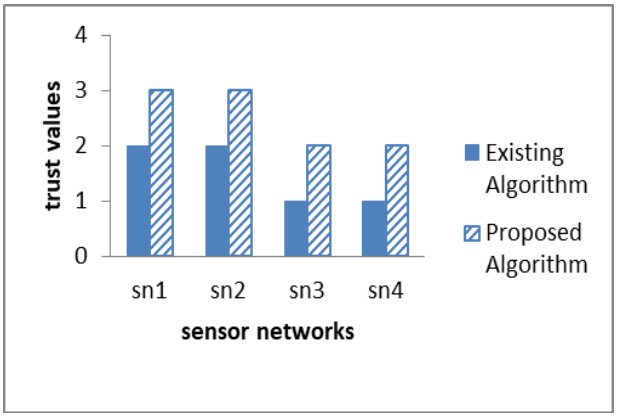

Fig.10. Sensor Data Transmission Trust values Vs various SNP's

Fig.10 shows Sensor Transmission trust values various SNP's the data leakage truest of the SNP's. Based on the usage of the data on SNP's by CSP's truest values of SN1 and SN2 are higher.

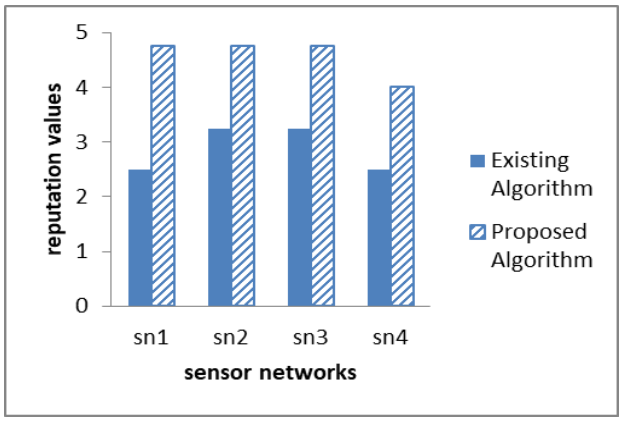

Fig.11. Reputation Values Vs various SNP's

Fig.11. shows the Reputation values of various SNP's is more for the proposed strategy as compared to the existing as within the proposed method. Feedback of the CSU's is utilized to calculate the Reputation esteem, using the feedback of its users about the service of SNP, CSP has to choose the derived SNP for its future service allocation. Hence SN1, SN2, SN3 will provide a better service than SN4.

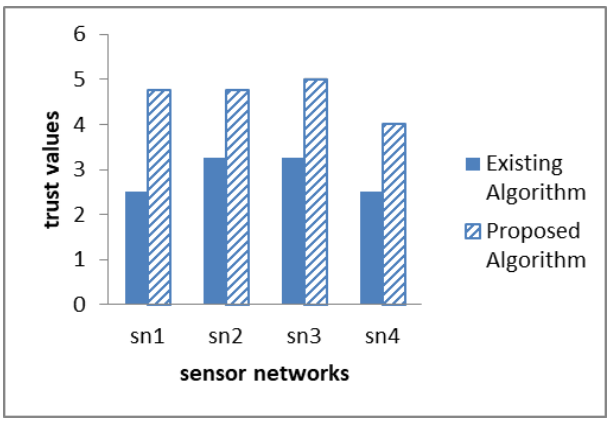

Fig.12. Trust values Vs various SNPs

Fig.12. shows trust values of different SNP's is more for the proposed method as compared to the existing as within the proposed method. Feedback of the CSU's is utilized to

calculate the trust value, and Feedback examination is done to evacuate wrong feedback and in this way increment the trust value of the veritable benefit providers as compared to others SN3 has higher believe values by since all cloud trust calculate values. Thus SN3 will be the alluring choice for getting to the service by its clients.

VII. CONCLUSIONS

The proposed system achieves the following functions for CC-WSN integration: 1) Authenticating CSU, CSP, and SNP. 2) Calculating trust and reputation regarding the service of CSP and SNP. 3) Helping CSU to choose desirable CSP and assisting CSP in selecting appropriate SNP. 4) Providing secure data to the users. Maintaining the security of the data stored on the cloud server is the main issue considered here. As there are numerous attacks on data stored on the cloud, the data needs to be secured by valid techniques. Here the encryption process is used for encrypting the data on the cloud, and the encrypted file will be accessed by users.

For calculating and maintaining of trust list and reputation list of organization, the feedback mechanism is employed. i.e., Feedback of each service from CSP to CSU and SNP to CSP is considered in the proposed algorithm for trust and reputation calculation that provide better trust and reputation value of CSP and SNP as compared to the existing method.

REFERENCES

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless Sensor Networks: A Survey,” *Computer Network Journal* vol. 38, no. 4, pp. 393–422, Mar. 2002.
2. M. Yuriyama and T. Kushida, “Sensor-Cloud Infrastructure -Physical Sensor Management with Virtualized Sensors on Cloud Computing,” in *13th International Conference on Network-Based Information Systems (NBiS)*, pp. 1–8, Sep 2010.
3. Q. Zhang, L. Cheng, and R. Boutaba, “Cloud Computing: State-of-Theart and Research challenges,” *Journal of internet services and applications*, vol. 1,no. 1, pp. 7–18, 2010.
4. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud Cmputing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th utility,” *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, Jun. 2009.
5. Buddesab,Thriveni J,Venugopal. "Trust model genetic node recovery based on cloud theory for underwater acoustic sensor network." *International Journal of Electrical & Computer Engineering* ,Vol. 9, no.5, pp. 3759-3771,2019.
6. Chunsheng Zhu, Hasen Nicanfar, Victor C. M. Leung, and Laurence T.Yang, “An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration”, *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, jan 2015.
7. Zhao, Liang, Shaocheng Qu, and Yufan Yi. "A Modified Cluster-head Selection Algorithm in Wireless Sensor Networks based on LEACH." *EURASIP Journal on Wireless Communications and Networking* 2018.1 (2018): 287.
8. Guangjie Han, Jinfang Jiang, Lei Shu , Jianwei Niu and Han-Chieh Chao,"Management and applications of trust in Wireless Sensor Networks: A survey." *Journal of Computer and System Sciences* 80, no. 3 (2014): 602-617.
9. Chunsheng Zhu,Victor C.M. Leung,Hai Wang,Wei Chen,and Xiulong Liu”, "Providing desirable data to users when integrating wireless sensor networks with mobile cloud." In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, vol. 1, pp. 607-614. IEEE, 2013.
10. Yuichiro Takabe,Katsuyoshi Matsumoto,Motoi Yamagiwa,and Minoru Uehara ,"Proposed sensor network for living environments using cloud computing." In *2012 15th International Conference on Network-Based Information Systems*, pp. 838-843. IEEE, 2012.
11. Yan Lindsay Sun,Zue Han,Wei Yu ,and K.J. Ray Liu,"A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks." In *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, pp. 1-13. IEEE, 2006.
12. Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, and Obaid Ur Rehman" "Comparison based analysis of different cryptographic and encryption techniques using message authentication code (mac) in wireless sensor networks (wsn)." *arXiv preprint arXiv:1203.3103* (2012).
13. Saurabh Kumar Garg, and Rajkumar Buyya. "Green cloud computing and environmental sustainability." *Harnessing Green IT: Principles and Practices* 2012 (2012): 315-340.
14. Anupam Das and Mohammad Mahfuzul Islam. "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems." *IEEE Transactions on Dependable and Secure Computing* 9, no. 2 (2011): 261-274.
15. Josep M. Pujol,Ramon Sangüesa, and Jordi Delgado, "Extracting reputation in multi agent systems by means of social network topology." In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, pp. 467-474. ACM, 2002.
16. Saurabh Ganeriwal and Mani B. Srivastava, "Reputation-based framework for high integrity sensor networks." *ACM Transactions on Sensor Networks (TOSN)* 4, no. 3 (2008): 1
17. Li, Jing, Zhitao Guan, Xiaojiang Du, Zijian Zhang, and Zhenyu Zhou. "A Low-latency Secure Data Outsourcing Scheme for Cloud-WSN." In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-6. IEEE, 2017.
18. Pujol JM, Ramon Sangüesa, and Jordi Delgado. "Extracting reputation in multi agent systems by means of social network topology." In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, pp. 467-474. ACM, 2002.
19. Sushmit Ruj,Milos Stojmenovic, and Amiya Nayak, "Decentralized access control with anonymous authentication of data stored in clouds." *IEEE transactions on parallel and distributed systems* 25, no. 2 (2013): 384-394.
20. Fortino G, Pathan M, and Di Fatta G, "BodyCloud: Integration of Cloud Computing and body sensor networks." In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, pp. 851-856. IEEE, 2012
21. V.Rajesh,J.M.Gnanasekar,R.S.Ponmagal,and.Anbalagan,‖Integration of Wireless Sensor Network with Cloud,‖ in International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), pp.321-323,2010.
22. Buddesab,Bhavyashree S P,Thriveni J, and Venugopal K R. "Integration of Wireless Sensor Network and Cloud Computing Using Trust and Reputation Technique." In Emerging Research in Electronics, Computer Science and Technology, pp. 69-82. Springer, Singapore, 2019.

AUTHORS PROFILE

Mr. Buddesab received the Bachelor of Engineering degree in Information Science and Engineering form The National Institute of Engineering Mysore, in 2009, and the Master of Technology in Computer Science and Engineering from M.S. Ramaiah Institute of Technology Bangalore, in 2013, both Visvesvaraya Technological University, Belgaum, India. He is currently working toward the PhD degree from Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, Bangalore University, India. His research interests include Cloud Computing, Scheduling and Resource Management, Data Security and Wireless Sensor Networks. He is a member of IEEE since 2014. He has published research papers in reputed international journals and conference. He has one years of teaching experience and 4 years of Research Experience

Dr.Thriveni J has completed Bachelor of Engineering, Masters of Engineering and Doctoral Degree in Computer Science and Engineering. She has 4 years of industrial experience and 23 years of teaching experience. Currently she is Professor in the Dept. of CSE, Universit

Visvesvaraya College of Engineering, Bangalore. She has over 90 research papers to her credit. She has produced four doctorate students and guiding 07 Ph.D Students. Her research interests include Networks, Data Mining and Biometrics.

Dr.K. R. Venugopal is currently the Vice Chancellor Bangalore University, Bengaluru. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bengaluru. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Micro-processor Programming, Mastering C?? and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE, ACM and ISTE.