Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 9, September -2016

ATRCM: Trust and Reputation on Service Provider of CC with WSN which used by CSUs

[1]Mr.Waghmare Shriharsh Shivaji, [2]Mr.Raiphale Akash Subhash, [3]Mr. Puri Mahesh Haridas

[1,2,3]*Computer Department, DYPIET, Ambi, Pune University.*

Abstract — *Instigated by joining the intense information stock, information preparing capacities of cloud computing (CC) and in addition universal information gathering capacity of wireless sensor network (WSNs), CC-WSN combination got a great deal of attention from both the academia and industry. However, verification and also trust and reputation computation and managing of cloud service provider (CSPs) and sensor network provider (SNPs) are two exceptionally basic and scarcely investigated issues for this new scenario which have common issues. To fill the gap, this paper proposes a novel validated trust and reputation computation and management (ATRCM) framework for CC-WSN integration. Considering the realness of CSP and SNP, the quality necessity of cloud service user (CSU) and CSP, the cost, trust, and reputation of the service of CSP and SNP, the proposed ATRCM framework accomplishes by assuming, 1) confirming CSP and SNP to maintain a strategic distance from pernicious pantomime attacks; 2) computation and managing trust and reputation with respect to the service of CSP and SNP; 3) helping CSU pick attractive CSP and helping CSP in selecting proper SNP. 4) Also, protection of CSUs. Point by point examination and outline as well as further usefulness assessment results are introduced to exhibit the adequacy of ATRCM, took after with framework security investigation.*

Keywords-: *Cloud, Sensor Networks, Integration, Authentication, Trust, Reputation.*

I. INTRODUCTION

1.1 Cloud Computing (CC):

Cloud computing (CC) is a model to empower convenient, on-interest system access to a mutual pool of configurable figuring resources (e.g., servers, systems, storage, applications, and service) that could be quickly provisioned, discharged with negligible management exertion or service supplier cooperation. CC is included by that clients can flexibly use the foundation (e.g., systems, servers, and, storage), stages (e.g., working platform and middleware services), and software (e.g., application programs) offered by cloud suppliers in an on-interest way-[7]. Not just the working expense and business dangers and also support the costs of administration suppliers can be significantly got down with CC, additionally the service scale can be developed on interest also, online simple access for users could be given profiting from CC-[7].

1.2 Wireless Sensor Networks (WSNs):

Besides, Wireless sensor network (WSNs) is systems comprising of spatially disseminated self-ruling sensors, which are equipped for detecting the physical or natural conditions (e.g., temperature, sound, vibration, weight, movement, and so on.)-[8]. WSNs are generally engaged due to their awesome potential in regions of civilian, industry also, military (e.g., forest fire recognition, example, with respect to backwoods fire discovery, since sensor end nodes can be deliberate, traffic observing, activity checking, war zone reconnaissance, and so on.), which could change the traditional path for individuals to associate with the physical world. For haphazardly, thickly sent in a forest fire, the accurate beginning of a wood flame can be transferred to the end clients before the wood fire turns wild without the vision of physical flame. Likewise, regarding combat zone reconnaissance, as sensors can be deployed to consistently monitor the state of basic landscapes, approach courses, ways and straits in a war zone, the exercises of the contradicting strengths can be nearly viewed by observation focus without the inclusion of physical scouts.

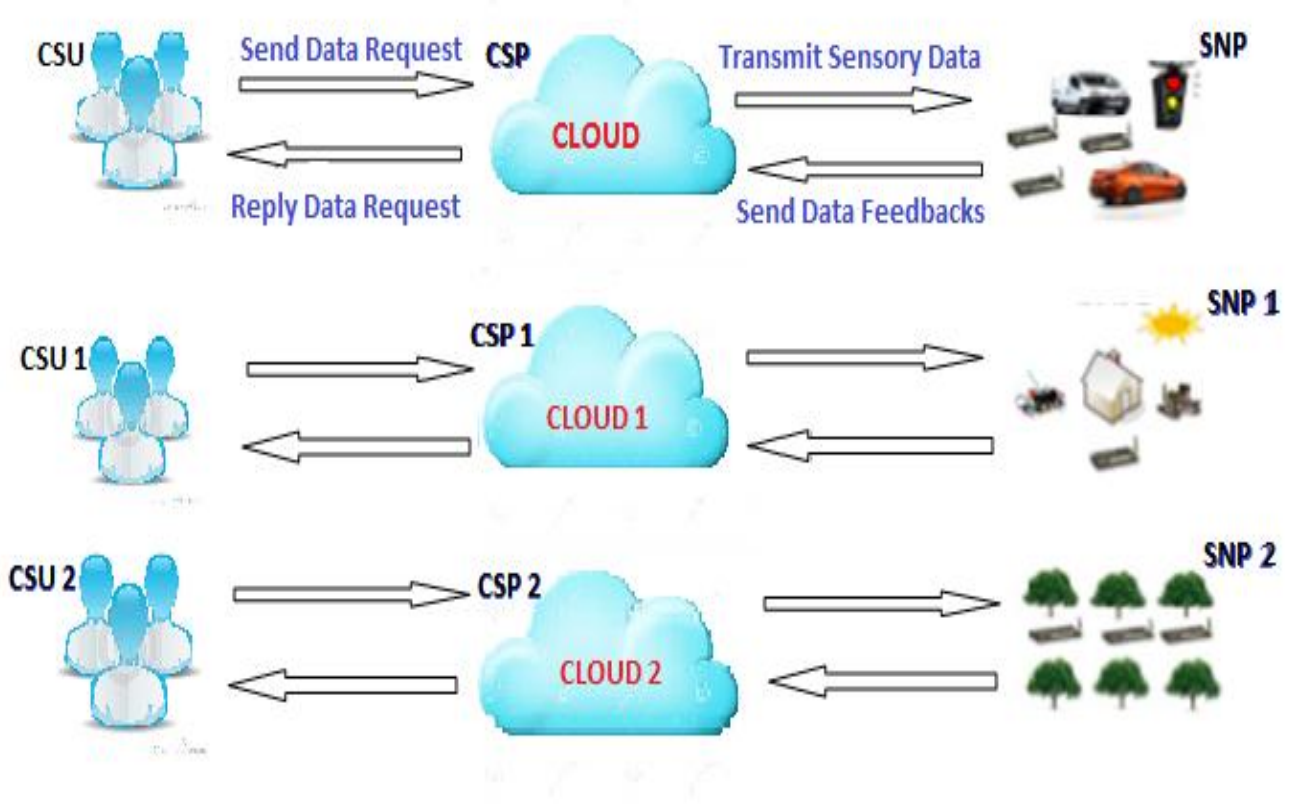

Figure 1. CC-WSN Integration

1.3 CC-WSN Integration

Incited by fusing the intense information storage and information handling capacities of CC and in addition the omnipresent information gathering ability of WSNs, CC-WSN mix got much consideration from both scholastic and modern groups. This combined issue is driven by the potential application situations appeared in Fig. 1. Specifically, sensor network provider (SNPs) gives the tangible information (e.g., activity, video, climate, dampness, temperature) gathered by the conveyed WSNs to the cloud service provider (CSPs). CSPs use the effective cloud to store and process the tangible information and after that further on interest offer the prepared tactile information to the cloud service user (CSUs) -[1] [2]. Subsequently CSUs can have entry to their required tactile information with only a straightforward customer to get to the cloud. In this common issue, SNPs are the information sources for CSPs, and CSUs go about as the information requesters for CSPs.

II. LITERATURE SURVEY

2.1 Providing desirable data to users when integrating wireless sensor networks with mobile cloud

Author: C. Zhu, V. C. M. Leung, H. Wang, W. Chen, and X. Liu. "Providing desirable data to users when integrating wireless sensor networks with mobile cloud". This paper proposes a novel framework for integrating WSNs and MCC. The proposed framework performs data recommendation, data prediction as well as data traffic monitoring in the cloud to obtain the data feature information required by the mobile users and potential status of WSNs. Then these user data feature information and potential WSNs status information are utilized to optimize the deployment of WSNs and check the status of WSNs. This could in turn offer the desirable data to the mobile users. Extensive evaluations also validate the effectiveness of the proposed framework.

2.2 Integration of cloud computing and body sensor networks

Author: G. Fortino, M. Pathan, and G. Di Fatta, "BodyCloud: Integration of cloud computing and body sensor networks," in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., Dec. 2012, pp. 851–856. This paper presents BodyCloud, a system architecture based on Cloud Computing for the management and monitoring of body sensor data streams. It incorporates key concepts such as scalability and flexibility of resources, sensor heterogeneity, and the dynamic deployment and management of user and community applications.

2.3 A trust evaluation model for QoS guarantee in cloud systems

Author: H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for QoS guarantee in cloud systems," Int. J. Grid Distribution Computation, vol. 3, no. 1, pp. 1–9, 2010.This paper presents a trust model for efficient reconfiguration and allocation of computing resources satisfying various user requests. Our model collects and analyzes reliability based on historical information on servers in a Cloud data center. Then it prepares the best available resources for each service request in advance, providing the best resources to users.

2.4 Trust management in cloud-integrated wireless sensor networks

Author: O. Savas, G. Jin, and J. Deng, "Trust management in the cloud-integrated wireless sensor networks," in Proc. Int. Conf. Collaboration Technology System, May 2013, pp. 334–341. In this paper, we first study the architecture of cloud-integrated WSNs, identify security challenges in this architecture, and then discuss how trust management could be effectively used to enhance the security of such a system.

2.5 A survey of attack and defense techniques for reputation systems

Author: K Hoffman, D Zage, C Nita-Rotaru - ACM Computing Surveys (CSUR), 2009.

Abstract Reputation systems provide mechanisms to produce a metric encapsulating Reputation for a given domain for each identity within the system. These systems seek to generate an accurate assessment in the face of various factors, including but not limited to.

III. RELATED WORK

In this segment, current works about the CC -WSN combination are checked on from the following two perspectives:

a. Authentication;

b. Trust and reputation.

3.1 Authentication

There are significant works with respect to authentication in the cloud. Case in point, a client authentication structure for CC is proposed in, going for giving ease of use, personality management, shared authentication also, session key assentation between the clients and the cloud server. Giving careful consideration to the light weight of verification since the cloud handles a lot of information in constant, demonstrates a lightweight multi-client validation plan taking into account cell automata in a cloud environment. Endorsement power based one-time secret key verification is used to perform validation. Supporting unknown validation, a decentralized access control plan for secure information storage in the cloud is exhibited in [3]. The proposed plan gives client denial, avoids replay assaults and in addition underpins creation, alteration and perusing information put away in the cloud. Watching the bad marks of losing rich data effectively and also the poor exhibitions coming about from the mind complex contributions of traditional unique mark acknowledgment approaches amid client verification by, it presents another unique mark acknowledgment plan in view of an arrangement of gathering geometric moment and Zernike moment components to verify clients in distributed computing interchanges. About verification in CC-WSN coordination, an extensible also, secure cloud engineering model for the sensor data framework is proposed in. It first describes the synthesis and the instrument of the proposed engineering model. At that point it advances security instrument for validating legitimate clients to get to sensor information and data service in the design, in view of an authentication power based Kerberos convention.

At last the model sending and reproduction test of the proposed engineering model are presented. Concentrating additionally on securing sensor information for sensor-cloud coordination frameworks by, a client verification plan is proposed by utilizing the multi-level verification procedure. It verifies the password in different levels for clients to get to cloud benefits in order to enhance validation level by request of greatness. Concerning the validation of the information produced by body sensor systems in, it shows, investigates and approves a down to earth, lightweight, robust information validation plan reasonable for cloud-based health observing. The fundamental thought is to use a Merkle hash tree to amortize computerized signature expenses and utilize system coding to recoup vital end nodes in the tree. Practical follows of typical working conditions demonstrate that more than 99% of the medical information can be verified at low overheads and taken a costly. To the best of our insight, current authentication plans in CC-WSN combination just concentrate on verifying clients or information. Unique in relation to these plans, our work concerns the authentication of CSPs and SNPs, which is a disregarded however essential issue in CC-WSN integration.

3.2 Trusts and Reputation

There are various works regarding trust or reputation of cloud. For instance, concentrating on the dependability of the cloud assets in, a system is proposed to assess the cloud resources dependability, by using an armoire to continually monitor and evaluate the cloud environment and in addition checking the assets the covering ensures. For productive reconfiguration and designation of distributed computing assets to meet different client asks for, a trust model which gathers and analyze the reliability of cloud assets in light of the chronicled data of servers is proposed in [2], so that the best accessible cloud resource to satisfy the client request can be set up ahead of time [3]. To decide the believability of trust feedbacks and additionally overseeing trust feedbacks in cloud situations, presents a structure named trust as services to enhance current trust management, by giving a versatile validity model with recognizing the validity and malicious inputs.

Examining the cloud responsibility issue in, it first uses criminologist controls to investigate the key issues to set up a trusted cloud and afterward gives a trust cloud system comprised of five reflection layers, where specialized and strategy based methodologies are connected to address responsibly. As for trust in the CC-WSN integration, the main related work is concentrating on how trusted could be successfully used to improve the security of a cloud integrated WSN. Especially, the security ruptures with respect to the information era, information transmission and in-system, preparing in the WSN coordinated with cloud is seen at first. At that point it demonstrates a few illustrations that trust can be utilized to perform trust-mindful information transmission and trust-mindful information preparing in the coordinated WSN and in addition trust-mindful administrations in the cloud or the best in class, there is no trust and reputation estimation and administration framework talking about CC-WSN reconciliation [4]. Our work is the principal framework computing and managing the trust and reputation in the situation of incorporating CC and WSNs further takes verifying CSPs and SNPs into consideration.

IV. SYSTEM ARCHITECTURE OF ATRCM

The system proposes an authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration.

Considering:

1. The authenticity of CSP and SNP.
2. The attribute requirement of cloud service user (CSU) and CSP.
3. The cost, trust and reputation of the service of CSP.

4.1 Existing System

WSNs are widely focused because of their great potential in areas of civilian, industrial and military (e.g., forest fire detection, industrial process monitoring, traffic monitoring, battlefield surveillance, etc.), which could change the traditional way for people to interact with the physical world.

For instance, regarding forest fire detection, since sensor nodes can be strategically, randomly, and densely deployed in a forest, the exact origin of a forest fire can be relayed to the end users before the forest fire turns uncontrollable without the vision of physical fire.

4.2 Disadvantages of Existing System

a. Security while authentication is less.
b. No trust over cloud.
c. Delay in accessing information.

4.3 Proposed System

To the best of our insight, there is no exploration, talking about and dissecting the authentication and additionally trust and reputation of CSPs and SNPs for CC-WSN mix. Filling this hole, this paper investigates the authentication of CSPs and SNPs and also the trust and reputation about the administrations of CSPs and SNPs. Further, this paper proposes a novel verified trusted and reputation computation and administration (ATRCM) framework for CC-WSN joins. Especially, considering (i) the realness of CSP and SNP; (ii) the quality necessity of CSU and CSP; (iii) the cost, trust and reputation of the administration of CSP and SNP, the proposed ATRCM framework accomplishes the accompanying three capacities:

a. Authenticating CSP and SNP to maintain a strategic distance from malignant pantomime assaults;
b. Calculating and overseeing trust and reputation in regards to the administration of CSP and SNP;
c. Helping CSU pick attractive CSP and helping CSP in selecting suitable SNP.

4.4 Advantages of Proposed System

a. There are different security policies for different domains.
b. The model considers the transaction context, the historical data of entity influences and the measurement of trust value dynamics.
c. The trust model is compatible with the firewall and does not break the firewall‘s local control policies.

V. EVALUATION OF SYSTEM FUNCTIONALITY

In this area, we assess whether our proposed ATRCM framework can satisfy the foreordained capacities: 1) validating CSP and SNP to maintain a strategic distance from malignant pantomime assaults; 2) ascertaining and overseeing trust and reputation with respect to the administration of CSP and SNP; 3) helping CSU pick attractive CSP and helping CSP in selecting suitable SNP, based on (i) the genuineness of CSP and SNP; (ii) the trait necessity of CSU and CSP and in addition (iii) the cost, trust what's more, reputation of the administration of CSP and SNP.

5.1 Assessment Setup

To play out the assessment, all the three pointed capacities are dissected in light of the flowcharts and procedures of the relating capacities. Especially, the third capacity is assessed using two delegate contextual investigations to illustrate the viability of ATRCM. Contextual investigation 1 includes a little amounts of CSUs, CSPs and SNPs, while contextual analysis 2 includes a substantial number of CSUs, CSPs and SNPs. The assessment procedures of the third capacity appeared in these two contextual analyses are all inclusive for CSUs, CSPs and SNPs with other properties and parameters.

5.2 Assessment Results

5.2.1 Authenticating CSP and SNP:

As for the authontecation of CSP and SNP, Part 1) verification flowchart of CSP and SNP appeared in Section III introduces the n nitty-gritty strides. In light of the flowchart, we can watch that if a malignant aggressor mimics the real CSP or real SNP, at that point it needs to possess the Certificate of CSP testament or the Certificate of SNP declaration in the first place. In the event that it can't give a declaration, then it is not a real association. Also, regardless of the possibility that the malevolent aggressor further an) offers a fake declaration (e.g., fake Certificate of CSP or fake Certificate of SNP) or b) gives a genuine yet denied declaration (e.g., denied Certificate of CSP or denied Certificate of SNP), despite everything it can't dispatch the pantomime assaults, since CSU and CSP check whether the mark of the testament is substantial and whether the testament is renounced. In this manner, we can accomplish that our proposed ATRCM framework is ready to anticipate vindictive pantomime assaults, by authorizing the CSP or SNP giving a legitimate authentication. In the meantime, as the legitimate authentication of CSP and SNP are acquired through ISO/IEC 27001 affirmation, the CSU will begin exchanging with CSP and CSP will start exchanging with SNP, with additional certainty and authontecation.

5.2.2 Calculating and Managing Trust and Reputation of Administration of CSP and SNP:

For the count and administration of trust and reputation as for the administration of the CSP furthermore, SNP, the nitty-gritty procedures are delineated in Section IV. Especially, count and administration of trust with respect to the administration of the CSP depend on cloud information handling trust, cloud information security trust and cloud information transmission trust. The base estimation of cloud information handling trust, security trust and transmission trust is the trust estimation of the administration of the CSP-[5]. Besides, the history that CSUs picked the administration of the CSP furthermore, the history that CSUs required the administration to get from a CSP are used to ascertain and deal with the reputation about the administration of the CSP-[6]. Besides, figuring and dealing with the trust of the administration of the SNP take sensor information accumulation trust, sensor system lifetime trust, sensor system reaction time trust and in addition sensor information transmission trust into record. The trust estimation of the administration of the SNP is the base estimation of sensor information accumulation trust, system lifetime trust, system reaction time trust and information transmission trust. At long last, the count and administration of the reputation of the administration of the SNP depend on the history that CSPs chose the administration of the SNP and the history that CSPs required the administration to get from a SNP.

VI. CONCLUSION

Here, Conclude that the system is calculated trust and reputation w.r.t CSP & SNP. So that, the system is properly gives security to respected data which is placed in cloud and network. Trust cost, reputation calculation mainly focusing on the CSP and SNP. Here in future, the system will be finding the authenticated user and manipulating the operations like sending request and receiving the proper data from CSP and SNP to authenticated user. If it misbehaves toward cloud then the system must be deactivate them as per the condition.

REFERENCES

[1] G. Fortino, M. Pathan, and G. DI Fatta, "BodyCloud: Integration of cloud computing and body sensor networks," in Proc. IEEE 4th Int. Conf. Cloud Computer Technology Sci., Dec. 2012, pp. 851–856.

[2] C. Zhu, V. C. M. Leung, H. Wang, W. Chen, and X. Liu, "Providing desirable data to users when integrating wireless sensor networks with mobile cloud," in Proc. IEEE 5th Int. Conf. Cloud Computer Technology, Science, Dec. 2013, pp. 607–614.

[3] H. Kim, H. Lee, W. Kim, and Y. Kim, "A trust evaluation model for QoS guarantee in cloud systems," Int. J. Grid, Distributed Computer, vol. 3, no. 1, pp. 1–9, 2010.

[4] O. Savas, G. Jin, and J. Deng, "Trust management in the cloud-integrated wireless sensor networks," in Proc. Int. Conf. Collaboration Technology System, May 2013, pp. 334–341.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Network, vol. 4, no. 3, May 2008, Art. ID 15.

[6] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Computer Survey, vol. 42, no. 1, Dec. 2009, Art. ID 1.

[7] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer System, vol. 25, no. 6, pp. 599–616, Jun. 2009.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw., Int. J. Comput. Telecommun. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

AUTHOR

MR. WAGHMARE SHRIHARSH SHIVAJI pursuing the Bachelor of Engineering Degree in Computer Engineering at Dr. D.Y. Patil Institute of Engineering and Technology, Ambi, Pune.

MR. RAIPHALE AKASH SUBHASH pursuing the Bachelor of Engineering Degree in Computer Engineering at Dr. D.Y. Patil Institute of Engineering and Technology, Ambi, Pune.

MR. PURI MAHESH HARIDAS pursuing the Bachelor of Engineering Degree in Computer Engineering at Dr. D.Y. Patil Institute of Engineering and Technology, Ambi, Pune.

