International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P) Volume-8, Issue-4, April 2018

A Secure System for Evaluation and Management of Authentication, Trust and Reputation in Cloud-Integrated Sensor Networks

Ms. Arati Phadtare, Prof. R. A. Deshmukh

***Abstract*— The data storing abilities of cloud computing (CC) and the data collecting ability of wireless sensor networks (WSNs) has influenced for the integration between the two. The cloud integrated sensor networks provide many opportunities for the researchers and the organizations by offering various computing services. However, the authentication and trust calculation of the Cloud Service Providers (CSPs) and Sensor Network Providers (SNPs) are important issues that have been hardly discussed for the CC-WSN integrated system. In this, an authenticated system for calculating trust value and reputation value for CSPs and SNPs is proposed. The proposed system authenticates CSP and SNP and helps the Cloud Service Users (CSUs) and CSPs in selecting appropriate CSP and SNP respectively. An Identity Manager (IDM) activates the registered users and Trust Manager (TM) calculates the trust and reputation values of CSPs and SNPs based on the feedbacks provided by CSUs and CSPs respectively. The analysis and the evaluation results show the effectiveness of the proposed system and prove that the system is secure against various attacks.**

***Index Terms*— Cloud providers, sensor network providers, feedback, authentication, trust, reputation.**

I. INTRODUCTION

Cloud computing depends on sharing a pool of resources, rather than installing local or personal hardware and software. The resources are retrieved from the internet through web-based tools and applications, instead of connecting directly to a server. The users can avail the services offered by the cloud as and when needed i.e. in an on-demand manner. Data and applications are stored in remote servers. Thus, users and businesses can use applications and access their personal files at any computer with an online connection, from anywhere and at any time. This allows for efficient computing by centralizing data storage and data processing.

A wireless sensor network (WSN) is a group of specialized sensors for monitoring and recording conditions at diverse locations. It has important applications such as environmental monitoring, traffic control application, weather monitoring, for detecting presence of vehicles, etc. The sensor nodes are distributed spatially and are equipped with wireless interfaces with the help of which they can communicate with one another to form a network.

Integrating cloud computing along with wireless sensor networks is a growing trend due to the enhancing capabilities of WSNs. This integration paradigm is shown in Fig. 1.

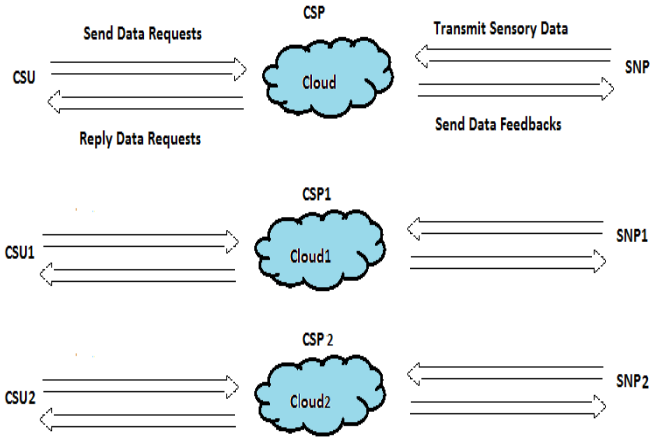


Fig.1.CC-WSN Integration

Sensor information system is a distributed information management system for collecting sensor data (e.g., traffic, weather, temperature, etc.) and effectively process, manage, and analyze the data generated from sensor networks. Cloud computing stores and processes such sensor data received from the sensor networks on further demand offers it to the end users. Users can thus access the required sensor data from the cloud with the help of a simple client.

Motivation

There are multiple online service provider options available to the cloud users now-a-days. These services have to be bought online. These services may be in the form of cloud service or in the form of sensor data. Hence, there should be some criteria on which users should be able to decide which service to choose. They promise discrete services yet fail to give up marking performance. Users also fall to these online traps due to lack of knowledge about the service providers. In this case, if user would have better knowledge about the service provider from a trusted entity then that will make a huge difference. Users will get only those services in which he is interested in and also will get better performance.

II. RELATED WORK

A. A Cloud Design for User-controlled Storage and Processing of Sensor Data [1]

This paper presents the architecture of a SensorCloud. The proposed security architecture imposes end-to-end data access control by the data owner from the sensor network to the Cloud storage. It also maintains isolation up to the

Ms. Arati Phadtare, Department of Computer Engineering, JSPM's R.S.C.O.E, Tathawade, Pune, India
Prof. R. A. Deshmukh, Department of Computer Engineering, JSPM's R.S.C.O.E, Tathawade, Pune, India

service-level. Thus, the security architecture allows the data owner to have a control over his data. The evaluation results show that the proposed SensorCloud architecture has effectively handles storage and memory overheads.

B. Strong User Authentication Framework for Cloud Computing [10]

This paper deals with a solid client validation system for cloud computing, where authenticity of the client is strongly validated before it gets into the cloud. This system presents common authentication scheme and also generates a session key between the clients and the cloud server. A client can change his private key in specific time intervals as requested. This protocol can prevent various attacks such as replay attack and denial of service attacks.

C. An Extensible and Secure Cloud Architecture Model for Sensor Information System [4]

This paper proposes cloud architecture for storing sensor data. The proposed security solution ensures the use of sensor data and information services and avoids illegal data breach in the cloud environment. A certificate authority (CA) based Kerberos protocol has been proposed to provide strong identity authentication. The architecture utilizes virtualization technology and cloud service functions that builds an extensible cloud environment which supplies scalable, flexible, reliable and secure sensor information services thereby solving the challenges faced by the present sensor information system. The experimental results show that the architecture provides high performance and stability throughout, while keeping scalability and flexibility brought by cloud.

D. Multi-Level Authentication in Sensor-Cloud Integration System [5]

This paper presents an authenticated system by applying the multiple levels of authentication techniques to secure the sensor data stored in the cloud. At various levels, a password is generated to access the data from cloud. Thus, the proposed system modeled using Petri nets helps in achieving strong authentication and authorization level.

E. Trust Management in Cloud-Integrated Wireless Sensor Networks [8]

The integrated system of cloud computing with sensor networks is prone to more security issues. The architecture of WSNs integrated with cloud is proposed. This paper identifies the security challenges in this architecture, and focuses on the effective use of trust management to strengthen the security of such a system. Trust management techniques should be designed carefully and the attacks against it should not be ignored.

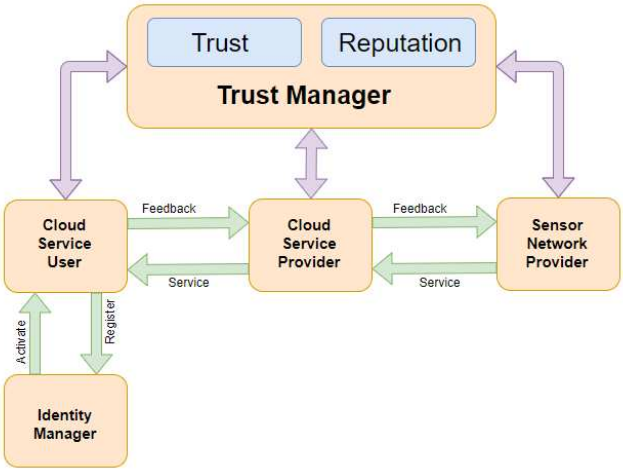
III. PROBLEM STATEMENT

To calculate Trust and Reputation values of CSPs and SNPs based on the feedbacks provided by the Cloud Service Users and the Cloud Service Providers respectively.

IV. IMPLEMENTATION DETAILS

A. System Architecture

The system architecture is represented in Fig.2.



a. Cloud Service User

Cloud Service Users (CSU) can get the services from multiple Cloud Service Providers. Users will first register to the Identity Manager. Identity Manager will activate the users. Once activated, users will use the services provided by Cloud Service Providers. The users will provide positive or negative feedbacks based on the service used of the selected CSP to the Trust Manager after the termination of service.

b. Cloud Service Provider

Cloud Service Providers (CSP) will activate the use of its services by respective users. CSPs can get the services from multiple Sensor Network Providers. CSPs will provide positive or negative feedbacks based on the service used of the selected SNP to the Trust Manager after the termination of service.

c. Trust Manager

The duty of Trust Manager (TM) is to calculate the trust values and reputation values of the Cloud and the Sensor Network Providers. The TM will activate if the received feedbacks from CSUs and CSPs are genuine. It will then update the trust and reputation values with the feedbacks received from CSUs and CSPs by using Natural Language Processing (NLP) technique. TM provides the values of trust and reputation as requested by CSUs or CSPs. The Trust Manager would thus prevent the system from various attacks. Without the TM there is possibility of giving false services to users.

d. Identity Manager

The duty of Identity Manager (IDM) is to activate the users that are registered to use the services of CSPs. It will audit if the registered users are genuine based on the mobile numbers provided. The trusted center entity would thus prevent fake users from registering which will result in preventing multiple attacks.

e. Sensor Network Provider

Sensor Network Providers (SNP) provides services to CSPs. It will activate its resources requested by the CSPs based on the availability.

B. *Algorithm*

- **AES Encryption**

The AES algorithm is a symmetric block cipher used to encrypt (encipher) and decrypt (decipher) information. It uses the same key for encrypting and decrypting, so both the sender and receiver must know and use of same secret key. AES as well as most encryption algorithms is reversible. The AES algorithm operates on bytes, which makes it simpler to implement and explain. AES is an iterated block cipher means that the same operations are performed many times on a fixed number of bytes.

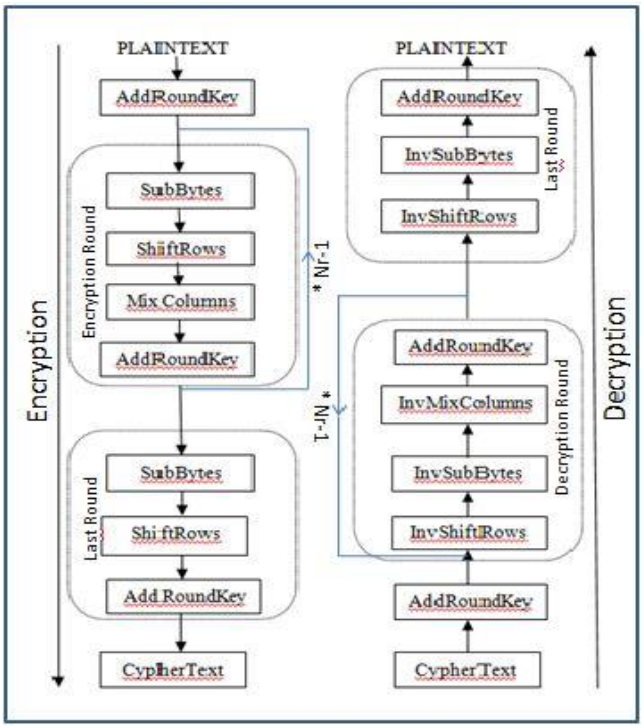


Fig.3.AES Encryption and Decryption

- **NLP (Natural Language Processing)**

Using NLP (Natural Language processing) we convert unstructured data to structured data using following method. The comments received from CSUs and CSPs are classified into Positive feedbacks (s) and Negative feedbacks (f) using the following steps: -

1. Tokenization
2. Stop Word Removal
3. Stemming
4. Classify (Positive sentence or Negative sentence)

Trust is calculated using the formula: T= {s + 1}/ {s + f + 2}

V. MATHEMATICAL MODEL

Let 'S' be the proposed system such that,
S = {CSU, CSP, TM, SNP, IDM}

C. *Input:*

CSU = {CSU1, CSU2 ,....,, CSUn}
CSP = {CSP1, CSP2, ……, CSPn}
SNP = {SNP1, SNP2, ..., SNPn}

Where,
CSU is Cloud Service User
CSP is Cloud Service Provider
TM is Trust Manager
IDM is Identity Manager
SNP is Sensor Network Provider

D. *Process Data:*

F is the function defined as:
F = {F1 (), F2 (), F3 (), F4 (), F5 (), F6 (), F7 ()}

F1(): CSUs will register to IDM and IDM will activate the users.

F2(): CSUs will purchase the services provided by CSPs and CSPs will purchase the networks from SNPs

F3(): CSPs and SNPs will activate the services used by CSUs and CSPs respectively

F4(): CSUs and CSPs will provide their feedbacks based on the services provided by CSPs and SNPs respectively

F5(): TM will activate the feedbacks received from CSUs and CSPs

F6(): TM will calculate Trust values of CSPs and SNPs

T_{cu} = {s + 1}/ {s + f + 2} ……. (1)

T_{kc} = {s + 1}/ {s + f + 2} …… (2)

F7(): TM will calculate Reputation values of CSPs and SNPs

$R_c = N/N_u$……. (3)

$R_k = N/N_u$……. (4)

Where,
s represents the (collective) amount of positive feedbacks provided by CSUs and CSPs

f represents the (collective) amount of negative feedbacks provided by CSUs and CSPs

T_{cu} is the trust value from CSP to CSU

T_{kc} is the trust value from SNP to CSP

R_c is the reputation value from CSP to CSU

R_k is the reputation value from CSU to SNP

N is the number of users that have used the services of CSPs and SNPs

N_u is the total number of users registered

E. *Output:*

The output will help the CSUs and CSPs to select the trusted services by selecting maximum trust and reputation values of CSPs and SNPs respectively.

VI. EXPERIMENTAL SETUP

The system is built using Java framework (version jdk1.8) on Windows platform. Eclipse is used as a development tool and database used is MySQL. The system doesn't require any specific hardware to run; any standard machine is capable of running the application.

VII. RESULTS AND DISCUSSION

Let us consider there are 4 CSPs and 4 SNPs that are providing services to the CSUs and CSPs respectively. Table 1 gives the trust and reputation percentages from CSPs to CSUs calculated by the TM based on the feedbacks using (1) and (3).

CSPs	Trust (%)	Reputation (%)
CSP1	60.00	53.33
CSP2	80.00	80.00
CSP3	77.78	73.33
CSP4	62.50	66.67

Table 1. Trust and Reputation calculation of CSPs

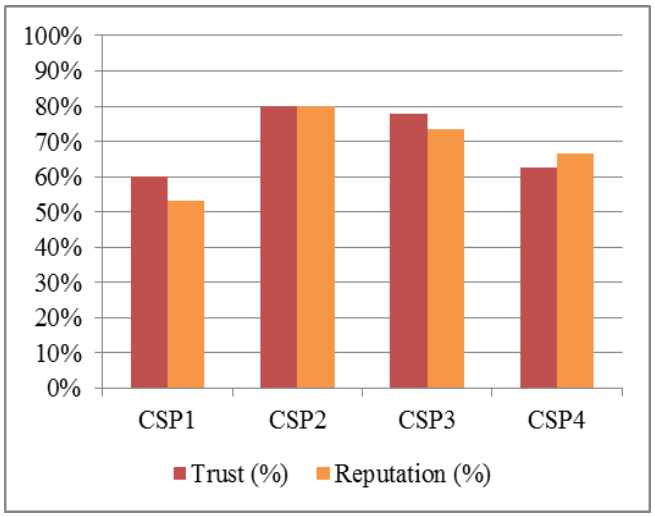


Fig.4. Trust and Reputation graph of CSPs

Table 2 gives the trust and reputation percentages from SNPs to CSPs calculated by the TM based on the feedbacks using (2) and (4).

SNPs	Trust (%)	Reputation (%)
SNP1	40.00	70.00
SNP2	40.00	62.50
SNP3	66.67	75.00
SNP4	50.00	50.00

Table 2. Trust and Reputation calculation of SNPs

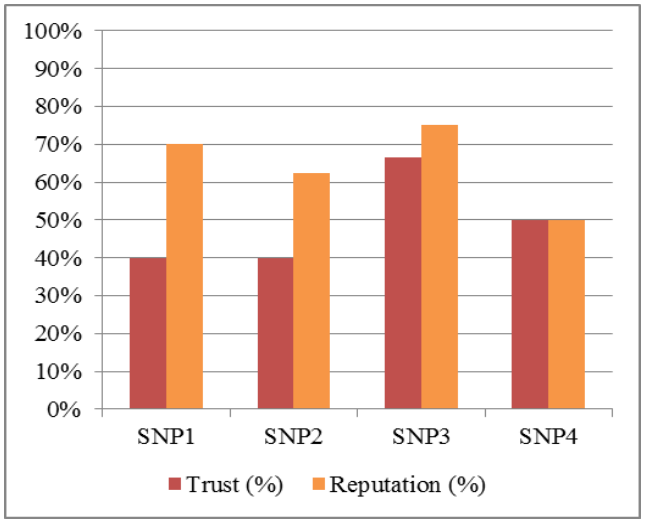


Fig.5. Trust and Reputation graph of SNPs

VIII. CONCLUSION

Thus, we have proposed a secure system which deals with the authentication, trust values and reputation values of CSPs and SNPs. This system will help the cloud users in selecting authentic and trustworthy CSP and will also assist the CSPs to choose appropriate SNP. The evaluation results show the effectiveness of the system. The security analysis proves that the system is immune against various attacks such as the collusion attack, good mouthing and the bad-mouthing attacks.

ACKNOWLEDGEMENT

The authors would like to thank the researchers as well as publishers for making their resources available. We would also like to thank teachers of RSCOE, Computer Engineering for their guidance and suggestions. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support.

REFERENCES

[1] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A cloud design for user-controlled storage and processing of sensor data," in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., Dec. 2012, pp. 232–240.

[2] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, "A survey on sensor-cloud: Architecture, applications, and approaches," Int. J. Distrib. Sensor Netw., vol. 2013, 2013, Art. ID 917923.

[3] S. Grzonkowski and P. Corcoran, "Sharing cloud services: User authentication for social enhancement of home networking," IEEE Trans. Consum. Electron., vol. 57, no. 3, pp. 1424–1432, Aug. 2011.

[4] P. You and Z. Huang, "Towards an extensible and secure cloud architecture model for sensor information system," Int. J. Distrib. Sensor Netw., vol. 2013, Jul. 2013, Art. ID 823418.

[5] H. A. Dinesha, R. Monica, and V. K. Agrawal, "Formal modeling for multi-level authentication in sensor-cloud integration system," Int. J. Appl. Inf. Syst., vol. 2, no. 3, pp. 1–6, May 2012.

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

[7] T. H. Noor and Q. Z. Sheng, "Trust as a service: A framework for trust management in cloud environments," in Proc. 12th Int. Conf. Web Inf. Syst. Eng., 2011, pp. 314–321.

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

[9] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Comput. Surv., vol. 42, no. 1, Dec. 2009, Art. ID 1.
[10] A. J. Choudhury, P. Kumar, M. Sain, H. Lim, and H. Jae-Lee, "A strong user authentication framework for cloud computing," in Proc. IEEE Asia-Pacific Services Comput. Conf., Dec. 2011, pp. 110–115.

ABOUT AUTHORS

Ms. Arati Phadtare received the B.E. degree in Information Technology from Vishwakarma Institute of Technology, under Pune University, India, in 2012. She is currently pursuing M.E. degree in Computer Science and Engineering from Rajarshi Shahu College of Engineering, Pune, India.

Prof. R. A. Deshmukh completed B.E. and M.E. in Computer Science and Engineering. She is pursuing PhD from Dr. Babasaheb Technological University, Lonere, Maharashtra. Her key research interests include Cloud Computing, NLP, Data Mining. She is currently working as Associate Professor in Rajarshi Shahu College of Engineering, Pune, India, Department of Computer Engineering with the total Experience of about 16 years