Scientific Journal of Impact Factor(SJIF): 3.134

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

International Journal of Advance Engineering and Research Development

Volume 2, Issue 11, November -2015

CC WSN:ATRCM for Powerful Data Storage and Processing

Santosh Aware[1] ,Haridas Lembhe[2] ,Guarav Gaikwad[3] ,Parshuram Late[4], Prof. Vikas Mapari[5]

[1-5]Department Of Computer Engineering,Dr.D.Y.PatilCollege Of Engineering, Ambi,Pune

Abstract — *The combination Cloud computing–Wireless sensor network has been pulling in the reasoning of numerous expert both in the college, school and the industry as it gives numerous opportunities for organizations by offering a scope of measure services, So information collection capability of wireless sensor networks (WSNs) turn out to be simple. For cloud computing to become generally use both the company and personally, several issues have to be solved. Regardless, authentication and also trust and position calculation and management of cloud service providers (CSPs) and sensor network suppliers (SNPs) are two particularly critical and almost explored issues for this new paradigm. To fill the gap, our paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) framework for CC-WSN combination or integration. Considering the authenticity of CSP and SNP, the attribute necessity of cloud service user (CSU) and CSP, the risk, trust, and reputation of the service of CSP and SNP, the proposed ATRCM structure fulfills the three capacities: 1) checking CSP and SNP to avoid malicious impersonate assaults; 2) computing and managing trust and reputation with the service of CSP and SNP; and 3) assisting CSU pick desirable CSP and helping CSP in selecting suitable SNP. Detailed analysis and outline as well as further usefulness evaluation result are presented to show the effectiveness of ATRCM, followed with system security analysis.*

.

Keywords:-CSP(Cloud Service Provider), CSU(Cloud Service User), ATRCM(novel authenticated trust and reputation calculation and management), SNP(Sensor Network Provider),WSNs(Wireless Sensor Networks).

I. INTRODUCTION

Computing is being transformed to a model consisting of services that are commoditized and conveyed in a way like traditional utilities, for example, water, electricity, gas, and telephony. In such a model, users access services in light of their prerequisites without respect to where the services are facilitated or how they are delivered. cloud computing (CC) is a model to enable convenient, on-demand network access for a shared pool of configurable processing resources (e.g., servers, networks, storage, applications, and services) that could be quickly provisioned and released with minimal management effort or service supplier interaction. Wireless sensor networks (WSNs) are networked system comprising of spatially appropriated distributed autonomous sensors, which are capable of sensing the physical or environmental conditions.

1)Cloud network:

Cloud networking is a new networking paradigm for building and managing secure private networks over the public Internet by utilizing global cloud computing infrastructure. In cloud networking, traditional network functions and services including connectivity, security, management and control, are pushed to the cloud and delivered as a service.

2)Sensors:

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A Sensor converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically. Let's explain the example of temperature. The mercury in the glass thermometer expands and contracts the liquid to convert the measured temperature which can be read by a viewer on the calibrated glass tube.

3)Types of sensors:

The sensors are classified into the following criteria:

1. Primary Input quantity (Measurand)
2. Transduction principles (Using physical and chemical effects)
3. Material and Technology
4. Property
5. Application

4)Advantages of sensor networks:

- Sensors networks allow a system to be extended from one with basic functions to one that can receive and act on data about the environment it operates in.

Sensors such as PIR detectors are relatively cheap if using wired versions.

II. LITERATURE REVIEW

1) Privacy Preserving Access Control with Authentication for Securing Data in Clouds

AUTHORS: Sushmita Ruj

we propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

2) Toward Secure and Dependable Storage Services in Cloud Computing

AUTHORS: Cong Wang

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e. the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

3. Fuzzy Keyword Search over Encrypted Data in Cloud Computing

AUTHORS: Jin Li

As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional search able encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only *exact* keyword search. That is, there is no tolerance of minor typos and format inconsistencies which, on the other hand, are typical user searching behavior and happen very frequently. This significant drawback makes existing techniques unsuitable in Cloud Computing as it greatly affects system usability, rendering user searching experiences very frustrating and system efficacy very low. In this paper, for the first time we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system us ability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when *exact* match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search.

4. Cryptographic Cloud Storage

AUTHORS: SenyKamara

We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage

5. Identity-Based Authentication for Cloud Computing

AUTHORS: Hongwei Li

Cloud computing is a recently developed new technology for complex systems with massive-scale services sharing among numerous users. Therefore, authentication of both users and services is a significant issue for the trust and security of the cloud computing. SSL Authentication Protocol (SAP), once applied in cloud computing, will become so complicated that users will undergo a heavily loaded point both in computation and communication. This paper, based on the identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes, presented a new identity-based authentication protocol for cloud computing and services. Through simulation testing, it is shown that the authentication protocol is more lightweight and efficient than SAP, specially the more lightweight user side. Such merit of our model with great scalability is very suited to the massive scale cloud.

III. SURVEY OF PROPOSED SYSTEM

In this project, we are explored the authentication as well as trust and reputation calculation and management of CSPs and SNPs which are two very critical and barely explored issues with respect to CC and WSNs integration. We proposed a novel ATRCM system for CC-WSN integration.The proposed ATRCM system achieves the following three functions for CC-WSN integration:

i) Authenticating CSP and SNP to avoid malicious impersonation attacks.

ii) Calculating and managing trust and reputation regarding the service of CSP and SNP.

iii) Helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP,In addition, our system security analysis powered by three adversary models showed that our proposed system is secure versus main attacks on a trust and reputation management system, such as good mouthing, bad mouthing, collusion and white-washing attacks, which are the most important attacks.

IV. PROPOSED ALGORITHM

A) Authentication flowchart of CSP and SNP:

Step 1: CSPs provide the certificate to CSU and CSU checks whether the signature of the certificate is valid and whether the certificate is revoked. CSU filters the CSPs that are not qualified.
Step 2: SNPs offer the certificate to CSP and CSP checks whether the signature of the certificate is valid and whether the certificate is revoked. CSP filters the SNPs that are not qualified.

B) Trust and reputation calculation and management between CSU and CSPs:

Step 1: CSU checks whether the characteristics of CSPs satisfy the attribute requirement of CSU. Filter the CSPs that are not satisfied.
Step 2: CSU issues requests to TCE and achieves the value of the service from CSP to the CSU. CSU checks whether the value is greater than or equal to the value. Filter the CSPs that are not satisfied.
$T_{cu} \geq T_{scu}$
Step 3: CSU issues requests to TCE and achieves the value of the service offered by the CSP. CSU checks whether the Rc value is greater than or equal to the value. Filter the CSPs that are not satisfied.
$R_c \geq R_{sc}$
Step 4: CSU calculates the value between CSC of CSP and DSP of CSU and checks whether the Cc value is within the range. Filter the CSPs that are not satisfied.

Step 5: CSU checks whether ctc is revoked and chooses the service offered by the CSP with the maximum Mc and informs TCE about signed SLA or PLA.

$$M_c = -\alpha_c \cdot \frac{C_c}{|C_{bc}|} + \beta_c \cdot T_{cu} + \gamma_c \cdot R_c$$

Step 6: CSU checks whether ctc is revoked before using the service from the CSP. CSU sends feedbacks about the service of the CSP to TCE (Trusted Center Entity) based on PLA (Privacy Level Agreement) and SLA(Service Level Agreement) after the termination of service. TCE stores and updates the value as well as the value.

3) Trust and reputation calculation and management between CSP and SNPs

Step 1: CSP checks whether the characteristics of SNPs satisfy the attribute requirement of CSP. CSP also checks whether the characteristics of SNP satisfy the attribute requirement of CSU. Filter the SNPs that are not satisfied.
Step 2: CSP issues requests to TCE and receives the value of the service from SNP to the CSP. CSP checks whether the value is more than or equal to the value. Filter the SNPs that are not satisfied.

$T_{kc} \geq T_{skc}$

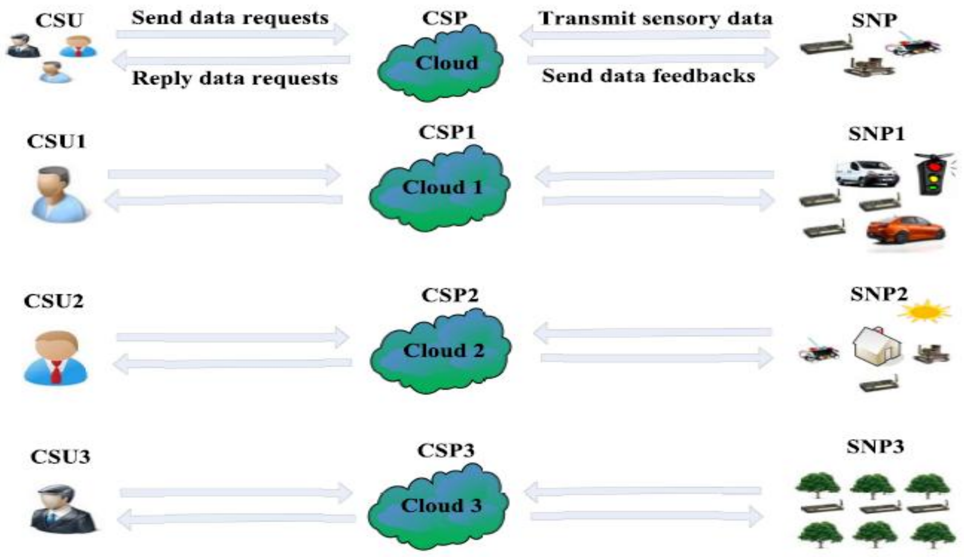
Step 3: CSP issues requests to TCE and receives the value of the service offered by the SNP. CSP checks whether the value is more than or equal to the value. Filter the SNPs that are not satisfied.

$R_k \geq R_{sk}$

Step 4: CSP calculates the value between SNSC of SNP and SNSP of CSP and checks whether the value is within the range. Filter the SNPs that are not satisfied
Step 5: CSP checks whether ctk is revoked and chooses the service offered by the SNP with the maximum Mk and informs TCE about signed SLA or PLA.

Step 6: CSP checks whether , is revoked before utilizing the service of the SNP. After the end of service, CSP sends feedbacks about the service of SNP to TCE based on SLA and PLA.
.

V. SYSTEM ARCHITECTURE



.

VI. CONCLUSION AND FUTURE WORK

We proposed a novel ATRCM system for CC-WSN integration. We explored the authentication as well as trust and reputation calculation and management of CSPs and SNPs, which are two very critical and barely explored issues with respect to CC and WSNs integration.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

REFERENCES

[1] Chunsheng Zhu, Victor C. M. Leung," 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, JANUARY 2015.
[2] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-theart and research challenges," *J. Internet Services Appl.*, vol. 1, no. 1, pp. 7–18, 2010. 130 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 1, JANUARY 2015
[3] 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 Generat. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, Jun. 2009.
[4] J. Baliga, R. W. A. Ayre, K. Hinton, and R. S. Tucker, "Green cloud computing: Balancing energy in processing, storage, and transport," *Proc. IEEE*, vol. 99, no. 1, pp. 149–167, Jan. 2011.
[5] K. M. Sim, "Agent-based cloud computing," *IEEE Trans. Services Comput.*, vol. 5, no. 4, pp. 564–577, Fourth Quarter 2012.
[6] 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.
[7] C. Zhu, L. Shu, T. Hara, L. Wang, S. Nishio, and L. T. Yang, "A survey on communication and data management issues in mobile sensor networks," *Wireless Commun. Mobile Comput.*, vol. 14, no. 1, pp. 19–36, Jan. 2014.
[8] M. Li and Y. Liu, "Underground coal mine monitoring with wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 5, no. 2, Mar. 2009,Art. ID 10.

AUTHORS

Santosh Aware, pursuing the B.E degree in Computer Engineering at Dr.D.Y.PatilCollege Of Engineering, Ambi,Pune.

Haridas Lembhe, pursuing the B.E degree in Computer Engineering at Dr.D.Y.PatilCollege Of Engineering, Ambi,Pune.

Guarav Gaikwad, pursuing the B.E degree in Computer Engineering at Dr.D.Y.PatilCollege Of Engineering, Ambi,Pune.

Parshuram Late, pursuing the B.E degree in Computer Engineering at Dr.D.Y.PatilCollege Of Engineering, Ambi,Pune

Prof. Vikas Mapari, pursuing the B.E degree in Computer Engineering at Dr.D.Y.PatilCollege Of Engineering, Ambi,Pune