

A

PROJECT REPORT

ON

**“Third Party Application for Providing Authentication Trust
and Reputation Calculation Management System in Cloud**

Computing & WSN Integration ”

*Project Submitted in partial fulfillment of
The requirement for the Award of Diploma in*

Computer Science & Engineering

Submitted to



Maharashtra State Board of Technical Education, Mumbai

Submitted by

Miss. Farisa Fatema Sd. Rizwan

Miss. Tejaswini N. Pathak

Miss. Shweta D. Rajput

Miss. Samruddhi J. Pol

Guided by

Mr. M.V. Shastri



Department of Computer Science & Engineering

Padm. Dr. V. B. Kolte College of Engineering and Polytechnic,

Malkapur Dist- Buldhana

2019-2020



**Padm. Dr. V. B. Kolte College of Engineering and
Polytechnic Malkapur, Dist: Buldhana
Department of Computer Science & Engineering**

CERTIFICATE

This is to certify that the final year project report on titled **“Third Party Application For Providing Authentication Trust & Reputation Calculation Management System For Cloud Computing & WSN Integration ”** is in partial fulfillment of the requirement for the award of diploma in Computer Science & Engineering affiliated to MSBTE completed by **Farisa Fatema Sd. Rizwan, Tejaswini N. Pathak ,Shweta D. Rajput, Samruddhi J. Pol** during the session 2019-2020.

Mr. M. V. Shastri
Project Guide

ACKNOWLEDGMENT

We feel profound pleasure in bringing out of this project report for which we have to go from pillar to post to make it a reality. This project work reflect contribution of many people with whom we had long discussion and without which it would not have been possible. We must first of all, express our thanks to our respected guide **Mr. M .V. Shastri** Department of computer science and engineering for providing us all required guidance to complete our project.

It would be unfair if we do not mention the invaluable contribution and timely co-operation extended to us by staff member of our department and especially we can never forget the worthiest advice given by **Mr. A. A. Maha** HOD Department of computer science and engineering that would help us the entire lifetime.

We are also very thankful to **Mr. S. N. Khachne** Principal of Padm. Dr. V.B. Kolte college of Engineering and Polytechnic Malkapur for co-operation and encouragement for collecting information and preparation.

I am extremely thankful to **Dr. A. W. Kharche** Director of Padm. Dr. V.B. Kolte college of Engineering and Polytechnic Malkapur for providing the infrastructure facilities to work in, without which this work would not have been possible.

Abstract

Induced by incorporating the powerful data storage and data processing abilities of cloud computing (CC) as well as ubiquitous data gathering capability of wireless sensor networks (WSNs), CC-WSN integration received a lot of attention from both academia and industry. However, authentication as well as trust and reputation calculation and management of cloud service providers (CSPs) and sensor network providers (SNPs) are two very critical and barely explored issues for this new paradigm. To fill the gap, this paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Considering the authenticity of CSP and SNP, the attribute requirement of cloud service user (CSU) and CSP, the cost, trust, and reputation of the service of CSP and SNP, the proposed ATRCM system achieves the following three functions: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; and 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP. Detailed analysis and design as well as further functionality evaluation results are presented to demonstrate the effectiveness of ATRCM, followed with system security analysis.

Or We can consider that 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.

Table of Content

Sr. No.	Title	Page No.
1	Chapter No 1	
	Introduction	03
2	Chapter No 2	
	Literature Survey	04-12
3	Chapter No 3	
	Scope and Objectives	13-18
4	Chapter No 4	
	Methodology	19-26
5	Chapter No 5	
	Details of Design, working and processes	27-31
6	Chapter No 6	
	Results	32-35
	Applications	36
7	Chapter No 7	
	Conclusion	37
	Future Scope	38
8	Reference	

Chapter No 1

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.

Furthermore, wireless sensor networks (WSNs) are networks consisting of spatially distributed autonomous sensors, which are capable of sensing the physical or environmental conditions (e.g., temperature, sound, vibration, pressure, motion, etc.) WSNs are widely focused because of their great potential in areas of civilian, industry 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. In addition, with respect to battlefield surveillance, as sensors are able to be deployed to continuously monitor the condition of critical terrains, approach routes, paths and straits in a battlefield, the activities of the opposing forces can be closely watched by surveillance centre without the involvement of physical scouts.

A. 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.

B. 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.

C. Types of sensors The sensors are classified into the following criteria:

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

D. Advantages of sensor networks

1. 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.

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

Induced by incorporating the powerful data storage and data processing abilities of CC as well as the ubiquitous data gathering capability of WSNs, CC-WSN integration received much attention from both academic and industrial communities. This integration paradigm is driven by the potential application scenarios shown in Fig. 1. Specifically, sensor network providers (SNPs) provide the sensory data (e.g., traffic, video, weather, humidity, temperature) collected by the deployed WSNs to the cloud service providers (CSPs). CSPs utilize the powerful cloud to store and process the sensory data and then further on demand offer the processed sensory data to the cloud service users (CSUs). Thus CSUs can have access to their required sensory data with just a simple client to access the cloud. In this new paradigm, SNPs are the data sources for CSPs, and CSUs act as the data requesters for CSP.

Chapter No. 2

Literature Survey

A Survey of Trust and Reputation Management Systems in Wireless Communications: Trust is an important concept in human interactions which facilitates the formation and continued existence of functional human societies. In the first decade of the 21st century, computational trust models have been applied to solve many problems in wireless communication systems. This cross disciplinary research has yielded many innovative solutions. In this paper, we examine the latest methods which have been proposed by researchers to manage trust and reputation in wireless communication systems. Specifically, we survey the state of the art in the application of trust models in the fields of mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and cognitive radio networks (CRNs). We classify the mainstream methods into natural categories and illustrate how they complement each other in achieving design goals. Major research directions are also outlined.

A. Privacy Preserving Access Control with Authentication for Securing Data in Clouds : By 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.

B. Toward Secure and Dependable Storage Services in Cloud Computing : By 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.

C. Fuzzy Keyword Search over Encrypted Data in Cloud Computing :

By 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 behaviour 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 usability 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.

D. Cryptographic Cloud Storage: By 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. **E. Identity-Based Authentication for Cloud Computing:** By 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.

Existing System:

Data has to traverse a longer path from its origin to the system and in the process can potentially be destroyed or modified by an attacker. This is referred as the fidelity problem.

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.

In this project, we evaluate whether our proposed ATRCM system can fulfil the predetermined functions: 1) authenticating CSP and SNP to avoid malicious impersonation attacks;

2) calculating and managing trust and reputation regarding the service of CSP and SNP; 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP, based on (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP as well as (iii) the cost, trust and reputation of the service of CSP and SNP

There are substantial works regarding authentication in cloud. For instance, a user authentication framework for CC is proposed in existing, aiming at providing user friendliness, identity management, mutual authentication and session key agreement between the users and the cloud server. There are a number of research works with respect to trust or reputation of cloud. For example, focusing on the trustworthiness of the cloud resources in a existing work, a framework is proposed to evaluate the cloud resources trustworthiness, by utilizing an armor to constantly monitor and assess the cloud environment as well as checking the resources the armor protects. About authentication in CC-WSN integration, an extensible and secure cloud architecture model for sensor information system is proposed in one of the existing system. It first describes the composition and mechanism of the proposed architecture model. Then it puts forward security mechanism for authenticating legal users to access sensor data and information services inside the architecture, based on a certificate authority based Kerberos protocol. Finally the prototype deployment and simulation experiment of the proposed architecture model are introduced

Proposed System :

According to researchers at Berkeley, trust and security is ranked one of the top 10 obstacles for the adoption of cloud computing. Indeed, Service-Level Agreements (SLAs). Consumers' feedback is a good source to assess the overall trustworthiness of

cloud services. Many researchers have identified the importance of trust management and suggest solutions to determine and

To the best of our knowledge, there is no research discussing and analyzing the authentication as well as trust and reputation of CSPs and SNPs for CC-WSN integration. Filling this gap, this paper analyzes the authentication of CSPs and SNPs as well as the trust and reputation about the services of CSPs and SNPs. Further, this paper proposes a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. Particularly, considering (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP; (iii) the cost, trust and reputation of the service of CSP and SNP, the proposed ATRCM system achieves the following three functions. Authenticating CSP and SNP: With respect to the authentication of CSP and SNP, Part 1) authentication flowchart of CSP and SNP presents the detailed steps. Based on the flowchart, we can observe that if a malicious attacker impersonates the authentic CSP or authentic SNP, then it needs to own the ctc certificate or the ctk certificate first. If it cannot provide a certificate, then it is not a genuine organization. In addition, even if the malicious attacker further a) offers a fake certificate (e.g., f ctc or f ctk) or b) provides a real but revoked certificate (e.g., rtc or rtk), it still cannot launch the impersonation attacks, since CSU and CSP check whether the signature of the certificate is valid and whether the certificate is revoked. Thus, we can achieve that our proposed ATRCM system is able to prevent malicious impersonation attacks, by enforcing the CSP or SNP providing a valid certificate. Meanwhile, as the valid certificate of CSP and SNP are obtained through ISO/IEC 27001 certification, the CSU will start trading with CSP and CSP will begin trading with SNP, with more confidence and assurance.

- There are different security policies for different domains.
- The model considers the transaction context, the historical data of entity influences and the measurement of trust value dynamically.
- This will overcome all the drawbacks of existing system.

A. Authentication

There are substantial works regarding authentication in cloud. For instance, a user authentication framework for CC is proposed in [18], aiming at providing user friendliness, identity management, mutual authentication and session key agreement between the users and the cloud server. Paying particular attention to the lightweight of authentication since the cloud handles large amounts of data in real-time, shows a lightweight multi-user authentication scheme based on cellular automata in cloud environment. Certificate authority based one-time password authentication is utilized to perform authentication. Supporting anonymous authentication, a decentralized access control scheme for secure data storage in clouds is presented. The proposed scheme provides user revocation, prevents replay attacks as well as supports creation, modification and reading data stored in the cloud. Observing the demerits of losing rich information easily as well as the poor performances resulting from the complex inputs of traditional fingerprint recognition approaches during user authentication by , it introduces a new fingerprint recognition scheme based on a set of assembled geometric moment and Zernike moment features to authenticate users in cloud computing communications. About authentication in CC-WSN integration, an extensible and secure cloud architecture model for sensor information system is proposed in . It first describes the composition and mechanism of the proposed architecture model. Then it puts forward security mechanism for authenticating legal users to access sensor data and information services inside the architecture, based on a certificate authority based Kerberos protocol. Finally the prototype deployment and simulation experiment of the proposed architecture model are introduced

B. Trust and Reputation

There are a number of research works with respect to trust or reputation of cloud . For example, focusing on the trustworthiness of the cloud resources in , a framework is proposed to evaluate the cloud resources trustworthiness, by utilizing an armor to constantly monitor and assess the cloud environment as well as checking the resources the armor protects. For efficient reconfiguration and allocation of cloud computing resources to meet various user requests, a trust model which collects and analyses the reliability of cloud resources based on the historical information of servers is proposed in , so that the best available cloud resources to fulfil the user

requests can be prepared in advance. To determine the credibility of trust feedbacks as well as managing trust feedbacks in cloud environments, presents a framework named trust as service to improve current trust managements ,by introducing an adaptive credibility model to distinguish the credible and malicious feedbacks. Discussing the cloud accountability issue in , it first uses detective controls to analyse the key issues to establish a trusted cloud and then gives a trust cloud framework consisted of five abstraction layers, where technical and policy-based approaches are applied to address accountability. With respect to trust in the CC-WSN integration, the only related work is focusing on how trust management could be effectively used to enhance the security of a cloud integrated WSN. Particularly, the security breaches regarding data generation, data transmission and in-network processing in the WSN integrated with cloud are observed in first. Then it shows some examples that trust can be employed to perform trust-aware data transmission and trust-aware data processing in the integrated WSN as well as trust-aware services in the cloud.

System Architecture:

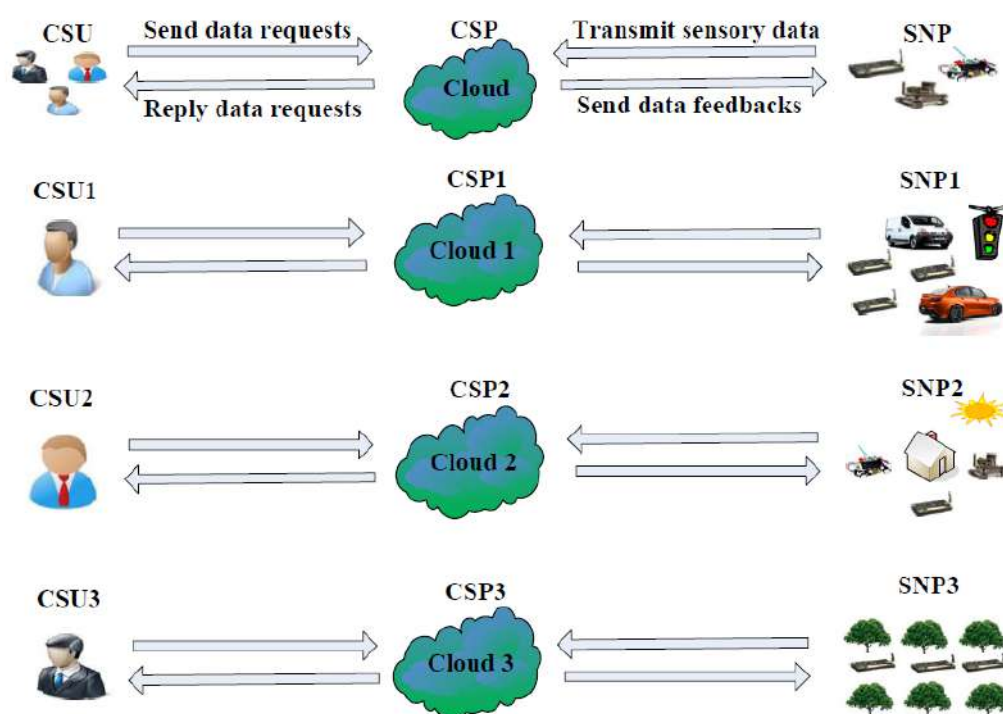


Figure.1. System Architecture

- 1. System Model:** There are multiple CSUs, CSPs and SNPs. Each CSU, CSP and SNP has several attributes. Particularly, the data service requested and required by the CSU owns the following attributes: data service pay (DSP); data type (DT); data size (DS); data request speed (DRS); data service time (DST). The cloud service provided and managed by each CSP has the following characteristics: cloud service charge (CSC); cloud operation cost (COC); sensor network service pay (SNSP); cloud service type (CST); cloud server number (CSN); cloud storage size (CSS); cloud processing speed (CPS); cloud operation time (COT).

2. Authentication of CSP and SNP:

In this module, we first develop the authentication of CSP and SNP. With that, we give some preliminaries about service level agreement (SLA) and privacy level agreement (PLA), followed with the preliminaries of trust and reputation and the preliminaries of trusted center entity (TCE). In this paper, as the key of our work is to enable CSU to choose the authentic and desirable CSP as well as assist CSP in selecting genuine and appropriate SNP, we focus on the authentication of CSP and SNP rather than the authentication of CSU. Specifically, the CSP needs to prove its authenticity to CSU and SNP has to show its authenticity to CSP. Generally, to evaluate trust from an entity (e.g., A or trustor) to another entity (e.g., B or trustee), A needs to gather evidence (e.g., honest, selfish, malicious behaviors), representing the satisfaction, about B either through direct interaction or information provided by third-parties.

3. Trust and Reputation of Service of CSP and SNP In this module, we can obtain that the fulfillment of service of CSP needs to receive and store the raw sensory data from SNP first. Then CSP processes the raw sensory data and stores the processed sensory data. Finally, CSP transmits the processed sensory data to CSU on demand. In this process, there are various types of trust (e.g., cloud data storage trust,

cloud data processing trust, cloud data privacy trust, cloud data transmission trust) which might concern the CSU to choose the service of CSP.

4. ATRCM system In this module, we implement the proposed authenticated trust and reputation calculation and management (ATRCM) system with Authentication flowchart of CSP and SNP; Trust and reputation calculation and management flowchart between CSU and CSPs; Trust and reputation calculation and management flowchart between CSP and SNPs.

Chapter No 3

Scope and Objectives

Scope & Objectives:

1. Authenticating CSP and SNP to avoid malicious impersonation attacks:

With respect to the authentication of CSP and SNP, Part 1) authentication flowchart of CSP and SNP presents the detailed steps. Based on the flowchart, we can observe that if a malicious attacker impersonates the authentic CSP or authentic SNP, then it needs to own the ctc certificate or the ctk certificate first. If it cannot provide a certificate, then it is not a genuine organization. In addition, even if the malicious attacker further a) offers a fake certificate (e.g., f ctc or f ctk) or b) provides a real but revoked certificate (e.g., rtc or rctk), it still cannot launch the impersonation attacks, since CSU and CSP check whether the signature of the certificate is valid and whether the certificate is revoked. Thus, we can achieve that our proposed ATRCM system is able to prevent malicious impersonation attacks, by enforcing the CSP or SNP providing a valid certificate. Meanwhile, as the valid certificate of CSP and SNP are obtained through ISO/IEC 27001 certification, the CSU will start trading with CSP and CSP will begin trading with SNP, with more confidence and assurance.

2. Calculating and managing trust and reputation regarding the service of CSP and SNP :

For the calculation and management of trust and reputation with respect to the service of the CSP and SNP, the detailed processes are illustrated. Particularly, calculation and management of trust regarding the service of the CSP are based on cloud data processing trust, cloud data privacy trust and cloud data transmission trust. The minimum value of $Tc1$, $Tc2$ and $Tc3$ is the trust value

of the service of the CSP. Moreover, the history that CSUs chose the service of the CSP and the history that CSUs needed the service to receive from a CSP are utilized to calculate and manage the reputation about the service of the CSP. Furthermore, calculating and managing the trust of the service of the SNP take sensor data collection trust, sensor network lifetime trust, sensor network response time trust as well as sensor data transmission trust into account. The trust value of the service of the SNP is the minimum value of Tk_1 , Tk_2 , Tk_3 and Tk_4 . Finally, the calculation and management of the reputation of the service of the SNP are based on the history that CSPs selected the service of the SNP and the history that CSPs required the service to receive from a SNP.

	C_c	T_{cu}	R_c	C_{bc}	T_{scu}	R_{sc}
$CSU_1 \leftrightarrow CSP_1$	-10	0.7	0.8	[-30, 30]	0.5	0.5
$CSU_1 \leftrightarrow CSP_2$	-15	0.8	0.7	[-30, 30]	0.5	0.5
$CSU_1 \leftrightarrow CSP_3$	-20	0.9	0.6	[-30, 30]	0.5	0.5
$CSU_2 \leftrightarrow CSP_1$	-15	0.7	0.8	[-30, 30]	0.5	0.5
$CSU_2 \leftrightarrow CSP_2$	-20	0.8	0.7	[-30, 30]	0.5	0.5
$CSU_2 \leftrightarrow CSP_3$	-25	0.9	0.6	[-30, 30]	0.5	0.5
$CSU_3 \leftrightarrow CSP_1$	-20	0.7	0.8	[-30, 30]	0.5	0.5
$CSU_3 \leftrightarrow CSP_2$	-25	0.8	0.7	[-30, 30]	0.5	0.5
$CSU_3 \leftrightarrow CSP_3$	-30	0.9	0.6	[-30, 30]	0.5	0.5

Table I. Parameters of CSUs and qualified CSPs

	C_k	T_{kc}	R_k	C_{bk}	T_{skc}	R_{sk}
$CSP_1 \leftrightarrow SNP_1$	-10	0.8	0.7	[-30, 30]	0.5	0.5
$CSP_1 \leftrightarrow SNP_2$	-15	0.7	0.6	[-30, 30]	0.5	0.5
$CSP_1 \leftrightarrow SNP_3$	-20	0.6	0.5	[-30, 30]	0.5	0.5
$CSP_2 \leftrightarrow SNP_1$	-15	0.8	0.7	[-30, 30]	0.5	0.5
$CSP_2 \leftrightarrow SNP_2$	-20	0.7	0.6	[-30, 30]	0.5	0.5
$CSP_2 \leftrightarrow SNP_3$	-25	0.6	0.5	[-30, 30]	0.5	0.5
$CSP_3 \leftrightarrow SNP_1$	-20	0.8	0.7	[-30, 30]	0.5	0.5
$CSP_3 \leftrightarrow SNP_2$	-25	0.7	0.6	[-30, 30]	0.5	0.5
$CSP_3 \leftrightarrow SNP_3$	-30	0.6	0.5	[-30, 30]	0.5	0.5

Table II. Parameters of qualified CSPs and SNPs

From the above analysis, we can obtain that the proposed ARTCM system is capable of calculating and managing the trust and reputation about the service of CSP and SNP.

3. Helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP : Regarding helping CSU to choose desirable CSP as well as assisting CSP in selecting appropriate SNP, Part 2) Trust and reputation calculation and management flowchart between CSU and CSPs and Part 3) Trust and reputation calculation and management flowchart between CSP and SNPs, present the detailed mechanisms to validate our demonstration. Specifically, we can see that the cost and trust as well as the reputation of the service of CSP and SNP are utilized for CSU and CSP to make the corresponding choice.

Case Study 1: In the following sample case study, there are three CSUs, four CSPs and five SNPs. With the filter process of the Step 1 of Part 2) and Part 3), we assume that one CSP and two SNPs are filtered out as their attributes do not satisfy the requirements. Then there are three CSUs, three CSPs and three SNPs, in which all characteristics of CSPs satisfy the attribute requirement of CSUs and all characteristics of SNPs satisfy the attribute requirement of CSPs. In the following, Table I shows the detailed parameters with respect to CSUs and qualified CSPs about C_c , T_{cu} , R_c , C_{bc} , T_{scu} and R_{sc} , which will be used from Step 2 to Step 5 of Part 2). And table II presents the detailed parameters regarding qualified CSPs and SNPs that will be utilized from Step 2 to Step 5 of Part 3) about C_k , T_{kc} , R_k , C_{bk} , T_{skc} and R_{sk} . Moreover, two typical weight sets about α_c , β_c , γ_c as well as α_k , β_k and γ_k are used to validate the effectiveness. In weight set 1, CSUs and CSPs take C_c , T_{cu} and R_c all into account. For weight set 2, CSUs and CSPs only consider one of C_k , T_{kc} and R_k .

	α_c	β_c	γ_c	Choice
CSU_1	1/3	1/3	1/3	CSP_3
CSU_2	1/2	1/4	1/4	CSP_3
CSU_3	1/5	2/5	2/5	CSP_3

Table III. Weight set of CSUs and corresponding choices

	α_k	β_k	γ_k	Choice
CSP_1	1/3	1/3	1/3	SNP_1
CSP_2	1/2	1/4	1/4	SNP_1
CSP_3	1/5	2/5	2/5	SNP_1

	α_c	β_c	γ_c	Choice
CSU_1	1	0	0	CSP_3
CSU_2	0	1	0	CSP_3
CSU_3	0	0	1	CSP_1

Table IV. Weight set 1 of qualified CSPs and corresponding choices

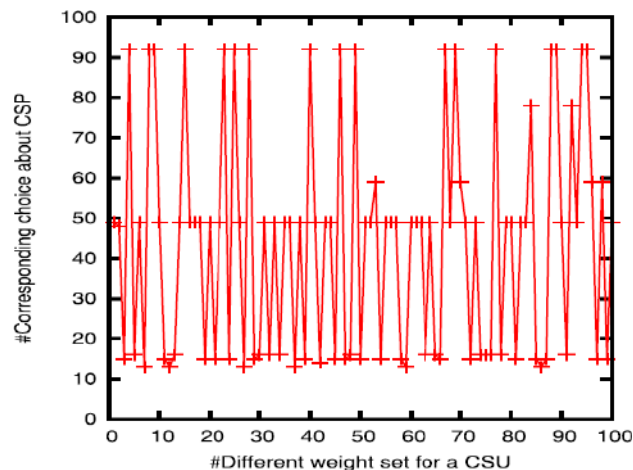
Table V. Weight set 2 of CSUs and corresponding choices

	α_k	β_k	γ_k	Choice
CSP_1	1	0	0	SNP_3
CSP_2	0	1	0	SNP_1
CSP_3	0	0	1	SNP_1

Table VI. Weight set 2 of qualified cps and corresponding choices

Weight set 1 of CSUs and the corresponding choices with respect to CSPs are shown in Table III. Meanwhile, weight set 1 of qualified CSPs and the corresponding choices with respect to SNPs are shown in Table IV. With, we can get that CSU_1 , CSU_2 and CSU_3 all choose CSP_3 as shown in Table III. In addition, CSP_1 , CSP_2 and CSP_3 all select SNP_1 as presented in Table IV. Furthermore, Table V and Table VI present weight set 2 of CSUs and the corresponding choices with respect to CSPs as well as

weight set 2 of qualified CSPs and the corresponding choices with respect to SNPs, respectively. Similarly, based on, we can obtain that *CSU1* and *CSU2* select *CSP3* while *CSU3* chooses *CSP1* as presented in Table V. Meanwhile, *CSP1* chooses *SNP3* while *CSP2* and *CSP3* both select *SNP1* as shown in Table VI. **Case Study 2:** In the following sample case study, there are one hundred CSUs, one hundred and fifty CSPs and two hundred SNPs. With the filter process of the Step 1 of Part 2) and Part 3), we suppose that fifty CSPs and one hundred SNPs are filtered out as their characteristics are not satisfied. Then there are one hundred CSUs, one hundred CSPs and one hundred SNPs, in which all characteristics of CSPs satisfy the attribute requirement of CSUs and all characteristics of SNPs satisfy the attribute requirement



of CSPs. In the following, the detailed parameters with respect to CSUs and qualified CSPs about C_c , T_{cu} , R_c , C_{bc} , T_{scu} and R_{sc} are randomly initialized and they will be utilized from Step 2 to Step 5 of Part 2). Similarly, the detailed parameters about qualified CSPs and SNPs are randomly initialized and

Fig.2. Different weight set for a CSU and Corresponding Choice about CSP.

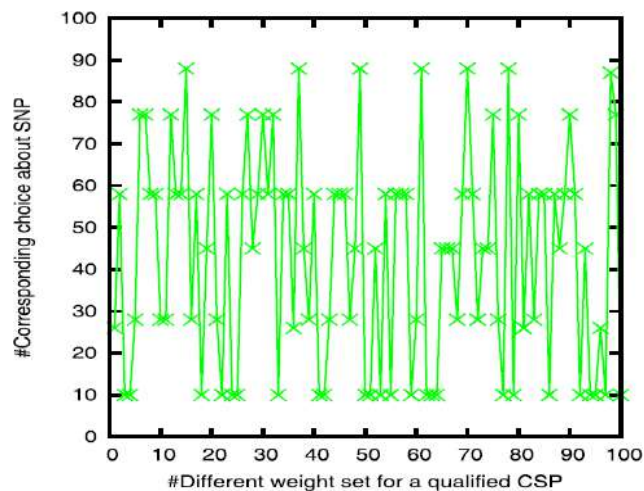


Fig.3. Different weight set for a qualified CSP and corresponding choice about SNP.

they will be used from Step 2 to Step 5 of Part 3) about C_k , T_{kc} , R_k , C_{bk} , T_{skc} and R_{sk} . In addition, one hundred different weight sets about α_c , β_c , γ_c as well as α_k , β_k and γ_k are randomly initialized to validate the effectiveness. Different weight sets for a CSU and the corresponding choices regarding CSPs are shown in Fig. 2. Meanwhile, different weight sets for a qualified CSP and the corresponding choices regarding SNPs are shown in Fig. 3. With, we can get that the CSU can choose CSP and CSP can choose SNP as shown in Fig. 2 and Fig. 3, respectively.

Chapter No 4

Methodology

Current works about the CC-WSN integration are reviewed from the following two aspects: (A) Authentication (B) Trust and reputation.

A. Authentication There are substantial works regarding authentication in cloud .For instance, a user authentication framework for CC is proposed in , aiming at providing user friendliness, identity management, mutual authentication and session key agreement between the users and the cloud server. Paying particular attention to the lightweight of authentication since the cloud handles large amounts of data in real-time, shows a lightweight multi-user authentication scheme based on cellular automata in cloud environment. Certificate authority based one-time password authentication is utilized to perform authentication. Supporting anonymous authentication, a decentralized access control scheme for secure data storage in clouds is presented in . The proposed scheme provides user revocation, prevents replay attacks

as well as supports creation, modification and reading data stored in the cloud. Observing the demerits of losing rich information easily as well as the poor performances resulting from the complex inputs of traditional fingerprint recognition approaches during user authentication by , it introduces

a new fingerprint recognition scheme based on a set of assembled geometric moment and Zernike moment features to authenticate users in cloud computing communications. About authentication in CC-WSN integration, an extensible and secure cloud architecture model for sensor information system is proposed in . It first describes the composition and mechanism of the proposed architecture model. Then it puts forward security mechanism for authenticating legal users to access sensor data and information services inside the architecture, based on a certificate authority based Kerberos protocol. Finally the prototype deployment and simulation experiment of the proposed architecture model are introduced.

Focusing also on securing sensor data for sensor-cloud integration systems by , a user authentication scheme is proposed by employing the multi-level authentication technique. It authenticates the password in multiple levels for users to access cloud services so as to improve authentication level by order of magnitude. Concerning the authentication of the data generated by body sensor networks in , it presents, analyzes and validates a practical, lightweight robust data authentication scheme suitable for cloud-based health-monitoring. The main idea is to utilize a Merkle hash tree to amortise digital signature costs and use network coding to recover strategic nodes within the tree. Experimental traces of typical operating conditions show that over 99% of the medical data can be authenticated at very low overheads and cost. To the best of our knowledge, current authentication Schemes in CC-WSN integration only focus on authenticating users or data. Different from these schemes, our work concerns the authentication of CSPs and SNPs, which is an ignored but important issue in CC-WSN integration.

B. Trust and Reputation

There are a number of research works with respect to trust or reputation of cloud .For example, focusing on the trustworthiness of the cloud resources in , a framework is proposed to evaluate the cloud resources trustworthiness, by utilizing an armor to constantly monitor and assess the cloud environment as well as checking the resources the armor protects. For efficient reconfiguration and allocation of cloud computing resources to meet various user requests, a trust model which collects and

analyses the reliability of cloud resources based on the historical information of servers is proposed in [10], so that the best available cloud resources to fulfil the user requests can be prepared in advance. To determine the credibility of trust feedbacks as well as managing trust feedbacks in cloud environments, [11] presents a framework named trust as service to improve current trust managements, by introducing an adaptive credibility model to distinguish the credible and malicious feedbacks. Discussing the cloud accountability issue in [12], it first uses detective controls to analyze the key issues to establish a trusted cloud and then gives a trust cloud framework consisted of five abstraction layers, where technical and policy-based approaches are applied to address accountability. With respect to trust in the CC-WSN integration, the only related work is focusing on how trust management could be effectively used to enhance the security of a cloud integrated WSN. Particularly, the security breaches regarding data generation, data transmission and in-network processing in the WSN integrated with cloud are observed in [13] first. Then it shows some examples that trust can be employed to perform trust-aware data transmission and trust-aware data processing in the integrated WSN as well as trust-aware services in the cloud. For the state of the art, there is no trust and reputation calculation and management system discussing CC-WSN integration. Our work is the first system calculating and managing the trust and reputation in the scenario of integrating CC and WSNs and also takes authenticating CSPs and SNPs into account.

IV. Authentication of csp and snp as well as trust and reputation of service of csp and snp : In this section, we first discuss the authentication of CSP and SNP. With that, we give some preliminaries about service level agreement (SLA) and privacy level agreement (PLA), followed with the preliminaries of trust and reputation and the preliminaries of trusted center entity (TCE). Finally, we discuss and analyze the trust and reputation with respect to the service of CSP and SNP respectively.

A. Authentication of CSP and SNP

In this project [14], as the key of our work is to enable CSU to choose the authentic and desirable CSP as well as assist CSP in selecting genuine and appropriate SNP, we focus on the authentication of CSP and SNP rather than the authentication of CSU. Specifically, the CSP needs to prove its authenticity to CSU and SNP has to show its

authenticity to CSP. Here, ISO/IEC 27001 certification , is applied to authenticate CSP and SNP, as it is an internationally recognized information security management system (ISMS) standard by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It requires that the information management of an organization (e.g., CSP or SNP) meets (i) the organization's information security risks are systematically examined; (ii) a coherent and comprehensive suite of information security controls is designed and implemented to solve those risks that are deemed unacceptable; (iii) an overarching management process is adopted to ensure that the information security controls continue to satisfy the organization's information security needs on an ongoing basis. Particularly, it provides confidence and assurance to trading clients of the organization, as the security status of the organization is audited to be qualified, by issuing a certificate with the ISO/IEC 27001 certification. After CSP and SNP are certificated with ISO/IEC 27001, they obtain the certificates (i.e., ctc and ctk) respectively

B. Preliminaries of SLA and PLA

An SLA, is a negotiated agreement between two or more parties, in which one is the customer and the others are service providers. In short, it is a part of a service contract, in which a service is formally defined. SLA specifies the levels of availability, serviceability, performance, operation and other attributes of the service. Usually, an SLA addresses the following segments about a service: definition, performance measurement, problem management, duties, warranties, termination. The subject of SLA is the result of the service received by the customer. An PLA is an agreement to describe the level of privacy protection that the CSP will maintain. Thus it is an appendix to the SLA between CSU and CSP. The SLA between CSU and CSP provides specific parameters and minimum levels on other performance (e.g., cloud processing speed, cloud operation time) of the cloud service,

while PLA addresses information privacy and personal data protection issues about the cloud service.

B. Preliminaries of Trust and Reputation Defined by Merriam Webster's Dictionary, trust is "assured reliance on the character, ability, strength or truth of someone or something" and reputation is "overall quality or character as seen or judged by people in general". However, trust and reputation are multidisciplinary concepts with different definitions and evaluations in various fields (e.g., psychology, sociology, economics, philosophy, wireless networks) [38]–[40]. For example, in the scenario of wireless communications, "Trust of a node A in a node B is the subjective expectation of node A receiving positive outcomes from the interaction with node B in a specific context". Also, "Reputation is the global perception of a node's trustworthiness in a network". Generally, to evaluate trust from an entity (e.g., A or trustor) to another entity (e.g., B or trustee), A needs to gather evidence (e.g., honest, selfish, malicious behaviours), representing the satisfaction, about B either through direct interaction or information provided by third-parties. With that, trustor (A) maps the gathered information from the evidence space to the trust space through a predefined mapping function and an aggregation function to obtain the trustworthiness value of trustee (B). Specifically, the trustworthiness obtained by mapping evidences from direct interaction is known as direct trust, while the trustworthiness achieved through mapping evidences from third-parties is indirect trust. Furthermore, a trustor can bring into account recent trust, which reflects only the recent behaviour's, as well as historical trust, which is built from the past experiences and it reflects long-term behavioural pattern. For instance, using indirect trust and historical trust helps trustor to protect trust evaluation (and trust system in general) from attacks such as good mouthing and bad mouthing, or sudden selfishness of a trustee. More discussion about these terms and definitions can be found in our references, for instance in [41]. In addition, to evaluate reputation about a trustee (e.g., B), the aggregated trust opinion of a group of entities are usually taken to represent the reputation value. A widely used way to map the observed information from the evidence space to the trust space is the beta distribution illustrated as follows. Let s and f represent the (collective)

amount of positive and negative feedbacks in the evidence space about target entity, then the trustworthiness t of a subject node is then computed as $t = \frac{s+1}{f+s+2}$

$$f + s + 2.$$

D. Preliminaries of TCE In this project, based on the five main roles (e.g., cloud customer, cloud provider, cloud broker, cloud auditor and cloud carrier) in CC [47], we assume that the role of the cloud auditor is assigned to TCE. Furthermore, we assume that TCE consists of multiple entities in various locations with a shared and secured database, e.g., in a data centre. Specifically, the duties of TCE are introduced as follows.

Duty 1) Receiving the copies of signed SLAs and PLAs from CSUs, CSPs and SNPs.

Duty 2) Receiving the feedbacks from CSUs about the services of CSPs and receiving the feedbacks from CSPs about the services of SNPs, based on signed SLAs and PLAs.

Duty 3) Auditing whether received copies are genuine as well as auditing whether received feedbacks that are to be utilized to calculate T_{cu} , T_{kc} , R_c and R_k are genuine, by security audit, privacy impact audit and performance audit, and etc.

Duty 4) Calculating and managing (i.e. storing and updating) T_{cu} , T_{kc} , R_c and R_k , with the genuine historical feedbacks received from CSUs about the services of CSPs and the genuine historical feedbacks from CSPs about the services of SNPs based on genuinely signed SLAs and PLAs.

Duty 5) Replying T_{cu} , T_{kc} , R_c and R_k values if these values are requested by CSUs or CSPs.

Duty 6) Auditing whether the T_{cu} , T_{kc} , R_c and R_k values received by CSUs and CSPs are genuine, by security auditing, privacy impact auditing and performance auditing, and etc.

Duty 7) Monitoring the process of the proposed ATRCM system to detect misbehaviours of CSUs, CSPs or SNPs that affect the process of ATRCM.

E. Trust of Service of CSP From Fig. 1, we can obtain that the fulfilment of service of CSP needs to receive and store the raw sensory data from SNP first. Then CSP processes the raw sensory data and stores the processed sensory data. Finally, CSP transmits the processed sensory data to CSU on demand. In this project, there are various types of trust (e.g., cloud data storage trust, cloud data processing trust, cloud data privacy trust, cloud data transmission trust) which might concern the CSU to choose the service of CSP. Furthermore, for various CSUs, the types of trust that they concern are different. In this paper, we assume that the following three types of trust about CSP concern the CSU to choose the service of CSP and we further show how they are calculated.

i) Cloud Data Processing Trust: This trust is related to whether cloud processes the raw sensory data with error. TCE has a database which dynamically stores the non-error number (i.e., $Sc1$) and error number (i.e., $Fc1$) of data processing of each service from CSP to the CSU in the history, with the feedbacks about the historical SLAs regarding the service. The trust value of cloud data processing trust (i.e., $Tc1$) is calculated by TCE via equation (1).

$$Tc1 = \frac{Sc1+1}{Fc1+Sc1+2} \quad (1)$$

ii) Cloud Data Privacy Trust: This trust is about whether the sensory data stored on cloud can be accessed by others. Based on the feedbacks about previous PLAs regarding the service, assume the number that the sensory data accessed by others with respect to each service from CSP to CSU in the history stored on TCE database is $Fc2$. As CSU is generally sensitive about the data privacy, the trust value of cloud data privacy trust (i.e., $Tc2$) is presented by TCE through equation (2)

$$Tc2 = \begin{cases} 1, & Fc2 = 0 \\ 0, & Fc2 > 0 \end{cases} \quad (2)$$

iii) Cloud Data Transmission Trust: This trust is with respect to whether the data transmission from CSP to CSU is successful. Using the feedbacks of previous SLAs regarding the service, with the success number (i.e., $Sc3$) and failure number (i.e., $Fc3$) of data transmission of each service from CSP to the CSU in the history on TCE database, the cloud data transmission trust (i.e., $Tc3$) is shown by TCE as per equation (3).

$$Tc3 = \frac{Sc3+1}{Fc3+Sc3+2} \quad (3)$$

In summary, with respect to Tcu value calculation, the trust value Tcu of each service from CSP to CSU is calculated by TCE with a combination function (i.e. CF) of three-dimensional trust (i.e., cloud data processing trust, cloud data privacy trust and cloud data transmission trust), as per equation (4).

$$Tcu = CF(Tc1, Tc2, Tc3) \quad (4)$$

Specifically, about CF , there are many different ways to combine multi-dimensional trust. For example, a probabilistic trust model based on the Dirichlet distribution to combine multi-dimensional trust is shown in [49], by estimating the probability that each contract dimension will be successfully fulfilled as well as the correlations between these estimates. In addition, an MeTrust model is presented in [50], enabling each user to choose a dimension as a primary dimension and put different weights on different dimensions for trust calculation. In this project, we assume that these three types of trust (i.e., cloud data processing trust, cloud data privacy trust and cloud data transmission trust) are considered with equal weight and then the minimum trust value in these three trust values is taken as Tcu , through equation (5).

$$Tcu = \text{Minimum}\{Tc1, Tc2, Tc3\} \quad (5)$$

F. Reputation of Service of CSP In this project, based on the feedbacks of previous SLAs about the service, we assume that if the CSU chose the service of the CSP, then it means that the CSU somehow trusted that CSP and decided to use the service of the

CSP. Let us assume that the number of CSUs that chose the service of the CSP is CN_c and the number of CSUs that needed the service to receive from a CSP is N_u ($N_u \leq Nu$). Then the reputation value (i.e., R_c) of the service of the CSU is calculated by TCE following [42], [43] via equation (6).

$$R_c = \frac{CN_c}{Nu} \quad (6)$$

G. Trust of Service of SNP :, we can also observe that the service of SNP requires the sensor nodes to be deployed first and then sense, store and process data to achieve data collection. At last, the collected sensory data are transmitted from SNP to the CSP. Similarly, in this paper, we assume that the following four kinds of trust about SNP consist of the trust of service of SNP in the above process.

Chapter No 5

Detail of Design Working and Processes

For Designing Purpose To Prepare the Frontend we use the JSP(Java Server Pages) and for the backend we use the mySql Server

Frontend JSP : **JavaServer Pages (JSP)** is a collection of technologies that helps software developers create dynamically generated web pages based on HTML, XML, SOAP, or other document types. Released in 1999 by Sun Microsystems, JSP is similar to PHP and ASP, but uses the Java programming language. To deploy and run JavaServer Pages, a compatible web server with a servlet container, such as Apache Tomcat or Jetty, is required.

Architecturally, JSP may be viewed as a high-level abstraction of Java servlets. JSPs are translated into servlets at runtime, therefore JSP is a Servlet; each JSP servlet is cached and re-used until the original JSP is modified.

JavaServer Pages can be used independently or as the view component of a server-side model–view–controller design, normally with JavaBeans as the model and Java servlets (or a framework such as Apache Struts) as the controller. This is a type of Model 2 architecture.

JSP allows Java code and certain predefined actions to be interleaved with static web mark-up content, such as HTML. The resulting page is compiled and executed on the server to deliver a document. The compiled pages, as well as any dependent Java libraries, contain Java bytecode rather than machine code. Like any other .jar or Java program, code must be executed within a Java virtual machine (JVM) that interacts with the server's host operating system to provide an abstract, platform-neutral environment. JSPs are usually used to deliver HTML and XML documents, but through the use of OutputStream, they can deliver other types of data as well.

The Web container creates JSP implicit objects like request, response, session, application, config, page, pageContext, out and exception. JSP Engine creates these objects during translation phase.

Java Server Pages (JSP) is a server-side programming technology that enables the creation of dynamic, platform-independent method for building Web-based applications. JSP have access to the entire family of Java APIs, including the JDBC API to access enterprise databases. This tutorial will teach you how to use Java Server Pages to develop your web applications in simple and easy steps. It is used to create dynamic web content. In this JSP tags are used to insert JAVA code into HTML pages.

Advantages of using JSP: -

- It does not require advanced knowledge of JAVA
- It is capable of handling exceptions
- Easy to use and learn

- It can tags which are easy to use and understand
- Implicit objects are there which reduces the length of code
- It is suitable for both JAVA and non JAVA programmer

Features of JSP:

- Coding in JSP is easy: - As it is just adding JAVA code to HTML/XML.
- Reduction in the length of Code: - In JSP we use action tags, custom tags etc.
- Connection to Database is easier:-It is easier to connect website to database and allows to read or write data easily to the database.
- Make Interactive websites: - In this we can create dynamic web pages which helps user to interact in real time environment.
- Portable, Powerful, flexible and easy to maintain: - as these are browser and server independent.
- No Redeployment and No Re-Compilation: - It is dynamic, secure and platform independent so no need to re-compilation.
- Extension to Servlet: - as it has all features of servlets, implicit objects and custom tags

Backend MySQL Server: MySQL is an open-source relational database management system (RDBMS) Its name is a combination of "My", the name of co-founder Wideness's daughter, and "SQL", the abbreviation for Structured Query Language.

MySQL is free and open-source software under the terms of the GNU General Public License, and is also available under a variety of proprietary licenses. MySQL was owned

Advantages of MySQL Server: -

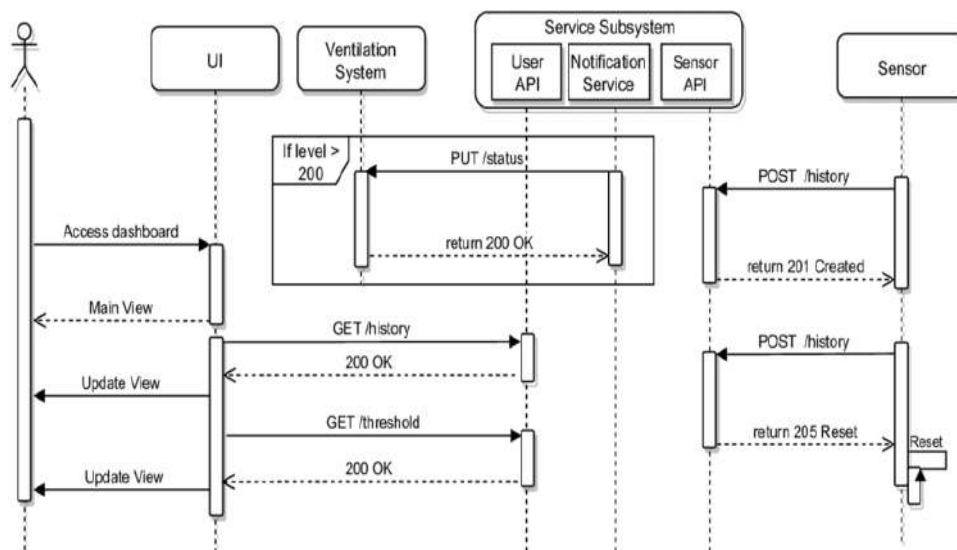
- Data Security.
- On-Demand Scalability.
- High Performance.
- Round-the-clock Uptime.
- Comprehensive Transactional Support. .
- Complete Workflow Control.

- Reduced Total Cost of Ownership.
- The Flexibility of Open Source.

MySQL database provides the following features:

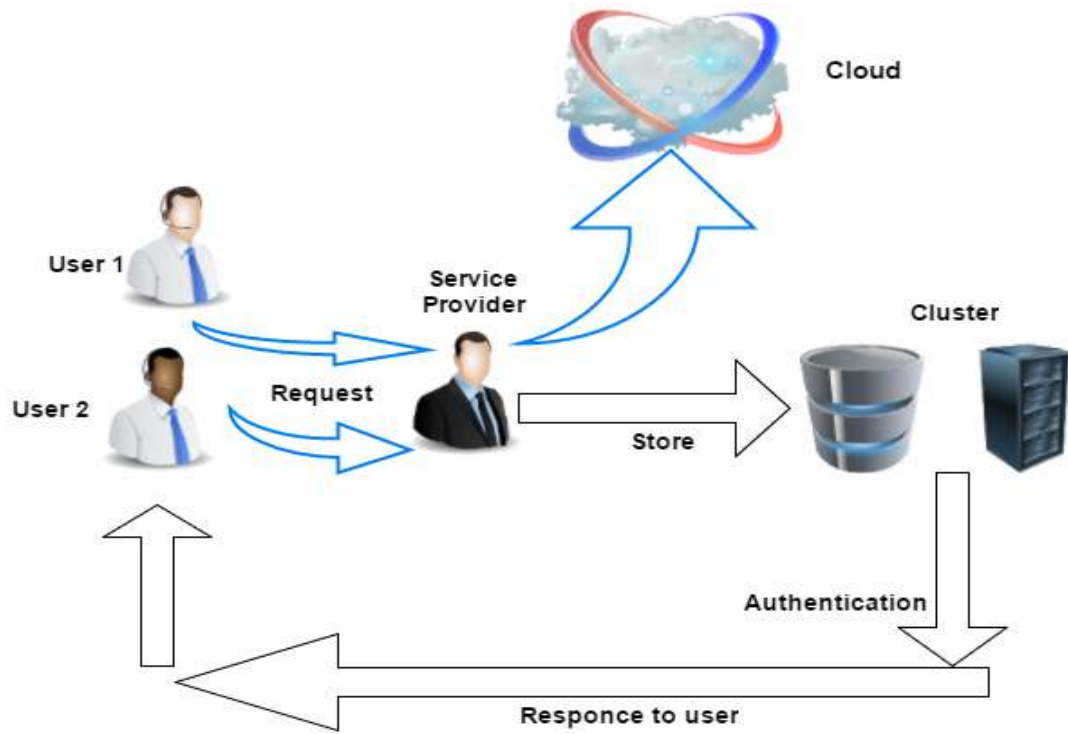
- High Performance and Scalability to meet the demands of exponentially growing data loads and users.
- Self-healing Replication Clusters to improve scalability, performance and availability.
- Online Schema Change to meet changing business requirements.
- Performance Schema for monitoring user- and application-level performance and resource consumption.
- SQL and No SQL Access for performing complex queries and simple, fast Key Value operations.
- Platform Independence giving you the flexibility to develop and deploy on multiple operating systems.
- Big Data Interoperability using MySQL as the operational data store for Hadoop and Cassandra.

Sequence Diagram :



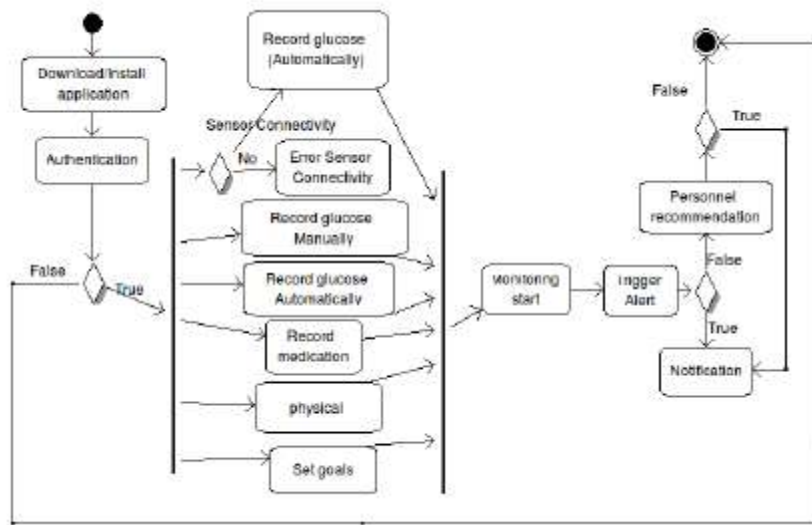
Third Party Application for Providing Authentication Trust and Reputation Calculation Management System in Cloud Computing and Wireless Sensor Network

Flow of the Project



Use Case Diagram :

Third Party Application for Providing Authentication Trust and Reputation Calculation Management System in Cloud Computing and Wireless Sensor Network

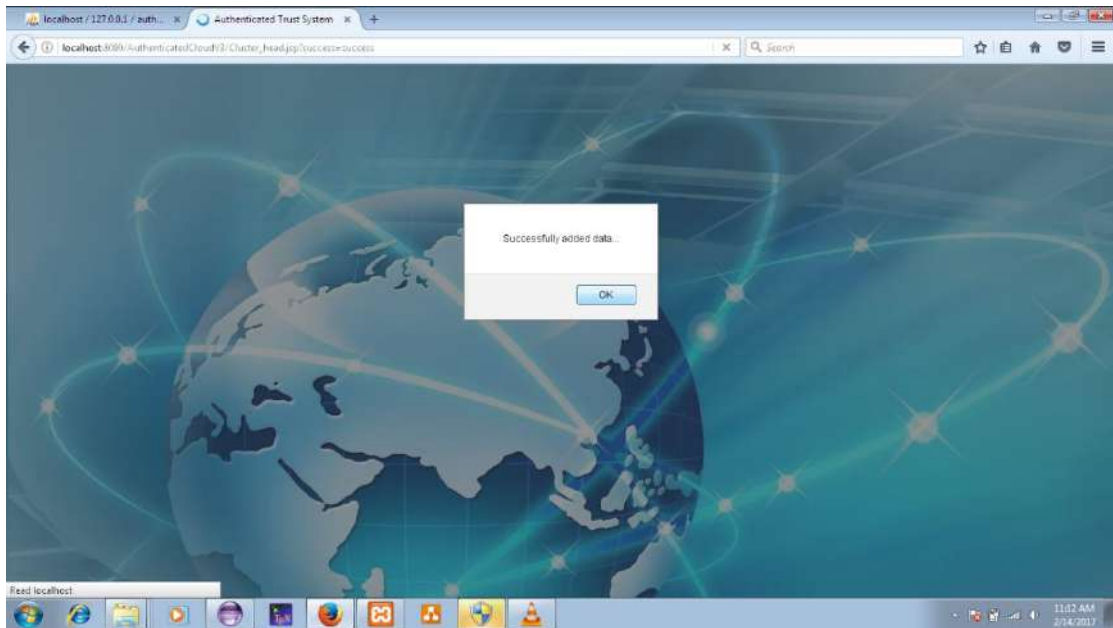


Chapter No: 6


Result and Application

Third Party Application for Providing Authentication Trust and Reputation Calculation Management System in Cloud Computing and Wireless Sensor Network

Result :



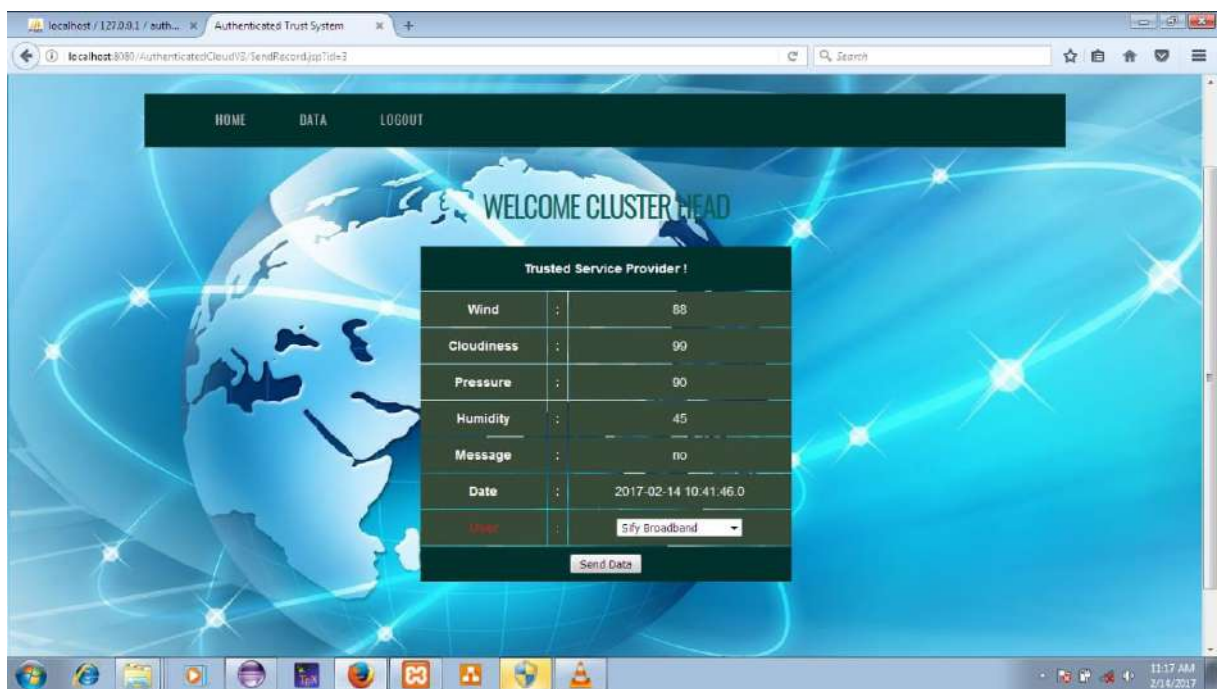
Third Party Application for Providing Authentication Trust and Reputation Calculation Management System in Cloud Computing and Wireless Sensor Network



The screenshot displays a web browser window with the URL `localhost:8080/AuthenticatedCloudV3/Cluster_head_data.jsp`. The page title is "AUTHENTICATED TRUST SYSTEM". A navigation bar contains "HOME", "DATA", and "LOGOUT". The main content area features a "NODE DATA" table with the following data:

Sr. No	Wind	Cloudiness	Pressure	Humidity	Added User	Message	Action
1	55	66	77	88	Node1	heavyrain	Already Sent
2	66	77	88	99	Node2	sunami	Already Sent
3	88	99	90	45	Node3	no	Send Data
4	66	77	88	99	Node1	sunami	Send Data
5	55	66	77	88	Node1	sunami	Send Data
6	66	77	88	99	Node2	heavyrain	Send Data
7	66	77	88	99	Node3	heavyrain	Send Data

Third Party Application for Providing Authentication Trust and Reputation Calculation Management System in Cloud Computing and Wireless Sensor Network



Third Party Application for Providing Authentication Trust and Reputation Calculation Management System in Cloud Computing and Wireless Sensor Network



Applications :

1. Cloud Provider –
 - a) Software as a Service (SAAS)
 - b) Platform as a Service (PAAS)
 - c) Infrastructure as a Service (IAAS)
2. Cloud Reseller -Google, IBM
3. Cloud Consumers
4. Cloud Based Service Provider
5. End Users
6. Business
7. Small Organizations
8. Environmental Monitoring for Emergency
9. Disaster Detection
10. Google Health
11. Telematics
12. Earth Observation
13. Wildlife Monitoring

Chapter No 7

Conclusion and Future Scope

Conclusion : In this project, we advancing 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. Further, we proposed a novel ATRCM system for CC-WSN integration. Discussion and analysis about the authentication of CSP and SNP as well as the trust and reputation with respect to the service provided by CSP and SNP have been presented, followed with detailed design and functionality evaluation about the proposed ATRCM system. All these demonstrated that the proposed ATRCM system achieves the following three functions for CC-WSN integration: 1) authenticating CSP and SNP to avoid malicious impersonation attacks; 2) calculating and managing trust and reputation regarding the service of CSP and SNP; 3) helping CSU choose desirable CSP and assisting CSP in selecting appropriate SNP, based on (i) the authenticity of CSP and SNP; (ii) the attribute requirement of CSU and CSP; (iii) the cost, trust and reputation of the service of CSP and 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. 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 in our case

Future Scope / Enhancement:

There are a few directions for our future work. We plan to combine different trust management techniques such as reputation and recommendation to increase the trust results accuracy. Performance optimization of the trust management service is another focus of our future research work.

Chapter No 8

References

- [1] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," *J. Internet Services Appl.*, vol. 1, no. 1, pp. 7–18, 2010.
- [2] 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.
- [3] 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.
- [4] K. M. Sim, "Agent-based cloud computing," *IEEE Trans. Services Comput.*, vol. 5, no. 4, pp. 564–577, Fourth Quarter 2012.
- [5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw., Int. Comput. Telecommun. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002.
- [6] 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.
- [7] 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.
- [8] M. Yuriyama and T. Kushida, "Sensor-cloud infrastructure—Physical sensor management with virtualized sensors on cloud computing," in *Proc. 13th Int. Conf. Netw.-Based Inf. Syst.*, Sep. 2010, pp. 1–8.
- [9] 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.

- [10] Y. Takabe, K. Matsumoto, M. Yamagiwa, and M. Uehara, "Proposed sensor network for living environments using cloud computing," in *Proc. 15th Int. Conf. Netw.-Based Inf. Syst.*, Sep. 2012, pp. 838–843.
- [11] R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A cloud design form user-controlled storage and processing of sensor data," in *Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci.*, Dec. 2012, pp. 232–240.
- [12] C. Zhu, V. C. M. Leung, L. T. Yang, X. Hu, and L. Shu, "Collaborative location-based sleep scheduling to integrate wireless sensor networks with mobile cloud computing," in *Proc. IEEE Globecom Workshops*, Dec. 2013, pp. 452–457.
- [13] 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 Comput. Technol. Sci.*, Dec. 2013, pp. 607–614.
- [14] 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.
- [15] 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.
- [16] M.-H. Guo, H.-T. Liaw, L.-L. Hsiao, C.-Y. Huang, and C.-T. Yen, "Authentication using graphical password in cloud," in *Proc. 15th Int. Symp. Wireless Pers. Multimedia Commun.*, Sep. 2012, pp. 177–181. [17] H. A. Dinesha and V. K. Agrawal, "Multi-dimensional password generation technique for accessing cloud services," *Int. J. Cloud Comput., Services Archit.*, vol. 2, no. 3, pp. 31–39, Jun. 2012.