REVIEWING AUTHENTICATED TRUST AND REPUTATION CALCULATION AND MANAGEMENT SYSTEMS FOR CLOUD AND SENSOR NETWORKS INTEGRATION: INSIGHTS, CHALLENGES, AND FUTURE DIRECTIONS

#1KOLIAPKA HARSHITHA,
#2N.SANTHOSH KUMAR, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: coming together to form something bigger overall Cloud computing and wireless sensor networks have enabled the provision of a wide range of computational services, sparked the interest of researchers and professionals in practically every industry. This is due to the fact that they provide a wide range of diverse business options. As a result, collecting data with WSNs is far less complicated than it was previously. Before individuals and businesses can fully adopt cloud computing, a number of challenges must first be solved. The issues of authenticating cloud service providers (also known as CSPs) and sensor network providers (commonly known as SNPs) in this new paradigm have received little attention in the academic literature. This research proposes a unique framework for calculating and controlling authenticated trust and reputation (ATRCM) in cloud computing and wireless sensor networks (CC-WSN). This framework will specifically address the management of ATRCM. The framework's goal is to provide a solution to a specific problem discovered in this domain. The ATRCM framework considers not only the attribute requirements of Cloud Service Users (CSUs) and CSPs, but also the price, trust, and reputation of the services provided by CSPs and SNPs, in order to fulfill its three purposes. This is done to make sure the framework is as complete as feasible. Validation of the CSP (Content Security Policy) and SNP (Sender Policy Framework) are critical components in combating phishing and other forms of fraudulent impersonation. Another critical aspect is evaluating and monitoring the market position of CSP and SNP services. It is critical to provide the Candidate Selection Unit (CSU) with the information they need to make informed decisions, as well as to assist the CSU in locating the appropriate Single Nucleotide Polymorphisms (SNPs) for the Candidate SNP Panel (CSP). This study lays forth a rigorous strategy and structure for doing in-depth research into ATRCM while also demonstrating its relevance and utility. For your convenience, the results of an examination of its supplemental features are offered here. Following that, the system's dependability is assessed.

KEYWORDS: Cloud computing, Sensor networks, Integration, Trustworthiness

1. INTRODUCTION

The paradigm that determines the distribution of computer resources has shifted significantly; the new method is more akin to the strategy used by traditional utilities such as water, electricity, gas, and telephones. This method assures that consumers, regardless of where they live or how the services are delivered, receive services that are specifically customized to their needs. Cloud computing (CC) allows you to acquire on-demand access to an external provider's resources (servers, networks, storage, applications, and services). CC stands for "cloud computing," and the phrase "user management" is intended to be used when referring to the coordination between service providers and their clients, which is an essential component for the efficient exploitation of these assets. WSNs deploy a network of self-contained sensors across an area to monitor and respond to changes in the environment.

Objectives:

➢ The use of CSP and SNP authentication

procedures reduces the risk of fraudulent impersonation attempts. The goal of this study is to identify and solve difficulties connected to the public's lack of trust in cloud-based SNPs and CSPs.

- Help the CSU and CSP choose the most qualified SNP and CSP.

2. LITERATURE SURVEY

A Survey of Trust and ReputationManagement Systems in WirelessCommunications

This research was written by Zhiqi Shen, Chunyan Miao, Dusit Niyato, Cyril Leung, and Han Yu.

Building and maintaining trust is important to the growth and survival of peaceful and flourishing human civilizations. To address the multiplicity of challenges presented by wireless networks at the turn of the century, experts turned to computational trust models. The extensive teamwork that went into this research resulted in the development of a wide spectrum of novel techniques. At the moment, the majority of research efforts are focused on the management of trust and reputation in WCNs. This article addresses the function of trust models in mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), and cognitive radio networks (CRNs), as well as the importance of trust models in each of these three types of networks. This study categorizes many design techniques and explains how they might be combined to achieve a variety of goals. We analyze in depth a number of potential future lines of inquiry within the scope of this work.

A survey on communication and data management issues in mobile sensor networks

The following people helped write the paper: Lei Shu, Takahiro Hara, Lei Wang, Shojiro Nishio, and Laurence T. Yang1.

Wireless sensor networks (WSNs) have sparked considerable interest since their beginnings in the late 1990s, owing to their utility in a wide range of military, commercial, and civilian sectors, including applications such as environmental and habitat monitoring. This is due in part to the fact that WSNs can be used in a variety of applications. The significance of Wireless Sensor Networks (WSNs) to the survival of the human race has grown in tandem with developments in processing power and data transfer speed. Because of the mobile nature of the sensors they connect, Wireless Sensor Networks (WSNs) pose network connectivity and endurance challenges. Wireless Sensor Networks (WSNs) that incorporate mobile sensors rather than stationary ones may see a rise in utility as a result of the growing number of use cases that require this. The development of wireless sensor networks (WSNs), which is impacted by a number of major factors that also drive the expansion of WSNs, influences the expansion of mobile wireless sensor networks (MWSNs). According to our observations, the researchers have not paid nearly enough attention to the challenges that arise with MWSN connectivity and data handling. The purpose of this research is to look into the methods used by mobile wireless sensor networks (MWSN) to handle the data and communications that occur within their systems at the moment. We also outline potential future research directions into MWSNs, with a focus on data management and transmission issues.

A Cloud Design for User-controlled Storage and Processing of Sensor Data

René Hummen, Klaus Wehrle, Daniel Catreiny, and Martin Henze all helped write the study.

The use of sensor networks and other pervasive sensing technologies enables the collection of massive volumes of data. The rate at which individuals use IoT devices will be directly proportional to the volume of data produced by these devices. It is expected that sensor data handling and storage will be straightforward in the cloud. One of the advantages of cloud computing is the ease with which data from many sources can be pooled and evaluated. Having said that, it is important to recognize that sensor data frequently contains private or secret information. The original owner of the data no longer has control over it once it has been uploaded to a cloud service. Concerns about one's own privacy, as well as legal ramifications, can all contribute to the building of hurdles that stymie the adoption process. In light of this, it is critical to build a cloud architecture that allows the data owner to control her private data while it is kept in the cloud in a dependable and safe manner. In this post, we will look at what it takes to build a dependable Cloud infrastructure and then present a summary of our results. In this response, we'll go over how SensorCloud's security was prioritized during development. Our suggested security architecture ensures total data ownership along the whole data flow, from the sensor network to the Cloud storage and processing subsystems. This is accomplished by the use of strict isolation requirements at the service level as well as end-to-end data access control. We will be able to examine the practicality and endurance of our cloud architecture by evaluating the first fully functional prototype. According to our findings, the proposed security architecture may be able to improve on features of the Cloud that are presently existent.

Secured Trust: A Dynamic Trust Computation Model for Secured Communication in Multi-Agent Systems

M. Anupam Das and M. M. The study's authors are Mahfuzul Islam and Mahfuzul Islam, both IEEE members and electrical and electronics engineers.

As the use of multi-agent systems grows more common, it is more vital than ever to handle data privacy and security problems in a timely manner. Because of its openness, anonymity, and rapid expansion, network applications such as pervasive computing, grid computing, and peer-to-peer (P2P) networks fall under the umbrella of multi-agent systems. Because of the qualities outlined above, multi-agent systems represent a possible risk to the efficiency of secure communication facilitation. Assessments of people's sincerity and integrity may be useful in decreasing risks by identifying those who can be trusted. Despite numerous attempts to build such a model, none have been successful in demonstrating trustworthiness in scenarios where hostile actors begin to behave in unexpected ways. It's likely that these models take too long to respond to changing adversary methods, but that's only a theory. The fair distribution of work among service providers is another component of multi-agent systems that is becoming increasingly crucial in the endeavor to sustain high-quality service delivery. When it comes to addressing this issue, the majority of trust and reputation models fall short. In this paper, a novel trust computation model known as "Secured Trust" is proposed in order to deal with hostile actors' adaptive behavior and provide a fair allocation of job opportunities among service providers. We study many aspects of trust evaluation in this article and propose a rigorous mathematical framework for determining whether or not a specific actor may be trusted. In addition, we provide a unique method for load balancing that makes use of the model's plethora of properties. The simulation findings show that our suggested strategy outperforms existing models in terms of effectively distributing labor resources among service-providing agents and accounting for antagonistic entities' deliberate changes in behavior.

A Survey of Attack and Defense Techniques for Reputation Systems

David Zage, Kevin Hoffman, and Cristina Nita-Rotaru were among those who contributed to the book's creation.

An individual's standing in a reputation system can be measured in a variety of ways. Despite the large number of individuals living there and the possibly hostile atmosphere, these methodologies make an effort to provide credible assessments. The fundamental goal of our research is to identify faults in existing reputational frameworks and to suggest possible solutions to these difficulties. We present a detailed analytical approach for assessing the current state of reputation management systems. The components of a reputation system and its features that are frequently the target of malevolent intent can be utilized to categorize the many types of cyberattacks on those systems. The purpose of this research is to look into how modern-day reputation management programs apply various types of disincentives. The study's conclusion is a complete review of a range of well-known P2P systems from both a favorable and detrimental standpoint. The purpose of this research is to determine which components of reputation systems are most vulnerable to assault, which countermeasures are most successful, and how to implement those precautions in real-world scenarios. The ultimate goal is to make future reputation management systems even more robust than they are now.

Existing System:

Wireless sensor networks, or WSNs, are rapidly gaining prominence as a result of their numerous applications in fields as diverse as the military, government, and industry. These networks have a wide range of uses, from monitoring business processes and tracking traffic to establishing early warning systems for forest fires and combat surveillance. As a result, they have the ability to change the status quo of how we now interact with our physical world, ushering in a new era with virtually endless possibilities. The intentional placement of tightly spaced sensor nodes within a forest allows users to acquire reliable information on the origin of a forest fire even when no fire is present.

Disadvantageous of Existing System:

- If there is an error in the process of identifying the user, the system's security is jeopardized. The length of time that passes between transmitting and receiving data after it has been transmitted.

3. SYSTEM ARCHITECTURE

This paper presents a novel technique for establishing and sustaining trust and reputation as a prerequisite for successfully merging cloud computing with wireless sensor networks (CC-WSN). Cloud service units (CSUs) and service level agreements (SLAs) are what distinguishes a cloud service provider (CSP) from other forms of internet service providers.

Consider the pricing of the service in light of its legitimacy, reputation, and history.

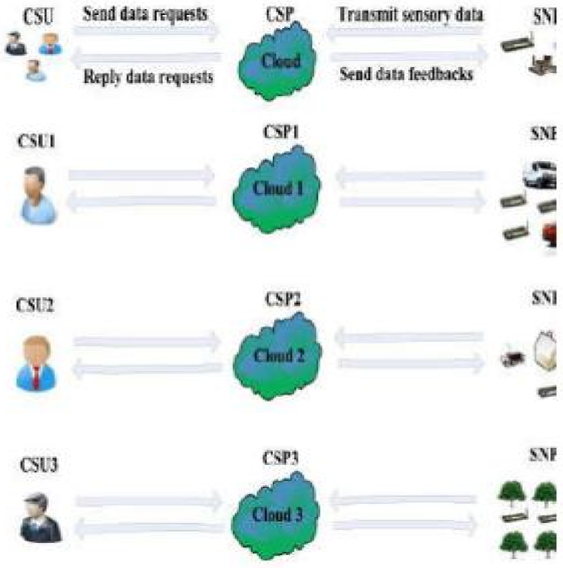

Fig1. The system's construction planning and execution

The SNP has been implemented into the proposed ATRCM system in order for it to achieve its many purposes. To prevent spoofing attacks, the identities of both the CSP and the SNP must be authenticated. Furthermore, it is in charge of assessing and monitoring the validity of the SNP and the CSP. One of the most critical steps in the process for the CSU to locate a competent CSP is to point a CSP in the direction of the right single nucleotide polymorphism (SNP).

Advantageous of Proposed System:

The method takes into account the history of previous trades as well as the influence of entities that existed in the past, and it performs an ongoing evaluation of the dependability measure.

The trust model has been proven to be compatible with the firewall as well as all of the criteria for local control.

4. CONCLUSION

A command and control wireless sensor network (CC-WSN) was combined with an advanced target identification and countermeasure system (ATRCM). Authentication, as well as the management and evaluation of trust and reputation for cloud service providers (CSPs) and sensor network platforms (SNPs), are two critical but often overlooked challenges associated with the integration of cloud computing (CC) and wireless sensor networks (WSNs).

REFERENCES

[1] Q. Zhang, L. Cheng, and R. Boutaba, “Cloud computing: State research challenges,” J. Appl., vol. 1, no. 1, pp. 7

[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] 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.

[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