IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 49-53

Enhance Searchable Public Key Encryption for Wireless Sensor Networks to Overcome Attacks

B.Raghupathi, R.Mohan Prakash, S.Prasanth, K.Mathanraj, Mrs.Revathi
UG Student, Final year CSE Department, Dhanalakshmi Srinivasan College of Engineering and Technology Mamallapuram, Kanchipuram District
Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi Srinivasan College of Engineering and Technology Mamallapuram, Kanchipuram District.

Abstract: *The industrial Internet of Things is flourishing, which is unprecedentedly driven by the rapid development of wireless sensor networks (WSNs) with the assistance of cloud computing. The new wave of technology will give rise to new risks to cyber security, particularly the data confidentiality in cloud-assisted WSNs (CWSNs). Search-able public-key encryption (SPE) is a promising method to address this problem. In theory, it allows sensors to up-load public-key ciphertexts to the cloud, and the owner of these sensors can securely delegate a keyword search to the cloud and retrieve the intended data while maintain-ing data confidentiality. However, all existing and semanti-cally secure SPE schemes have expensive costs in terms of generating ciphertexts and searching keywords. Hence, this paper proposes a lightweight SPE (LSPE) scheme with semantic security for CWSNs. LSPE reduces a large number of the computation-intensive operations that are adopted in previous works; thus, LSPE has search performance close to that of some practical searchable symmetric encryp-tion schemes. In addition, LSPE saves considerable time and energy costs of sensors for generating ciphertexts. Fi-nally, we experimentally test LSPE and compare the results with some previous works to quantitatively demonstrate the above advantages.*

I. Introduction

Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. It is noted that data owners lose ultimate control over the fate of their outsourced data; thus, the correctness, availability and integrity of the data are being put at risk. On the one hand, the cloud service is usually faced with a broad range of internal external adversaries, who would maliciously delete or corrupt users' data.

1.1 OBJECTIVE

To fully ensure the data integrity and save the users' computation resources as well as online burden, we propose a public auditing scheme for the regenerating-code-based cloud storage, in which the integrity checking and regeneration are implemented by a third party Auditor and a semi-trusted proxy separately on behalf of the data owner.

1.2 OVERVIEW

Trust management is one in all the foremost difficult problems for the adoption and growth of cloud computing. The highly dynamic, distributed, and non-transparent nature of cloud services introduces many difficult problems like privacy, security, and handiness. protective consumers' privacy isn't a simple task thanks to the sensitive info concerned within the interactions between customers and therefore the trust management service. protective cloud services against their malicious users (e.g., such users might provide dishonest feedback to disadvantage a specific cloud service) may be a tough downside. Guaranteeing the provision of the trust management service is another vital challenge owing to the dynamic nature of cloud environments. during this article, we describe the planning and implementation of Cloud Armor, a reputation-based trust management framework that has a group of functionalities to deliver Trust as a Service (TaaS), which has i) a completely unique protocol to prove the quality of trust feedbacks and preserve users' privacy, ii) associate degree adaptation and sturdy quality model for activity the quality of trust feedbacks to shield cloud services from malicious users and to match the trait of cloud services, associate degreed iii) an handiness model to manage the availability of the redistributed implementation of the trust management service. The practical and advantages of our approach have been valid by a example and experimental studies employing a assortment of real-world trust feedbacks on cloud services.

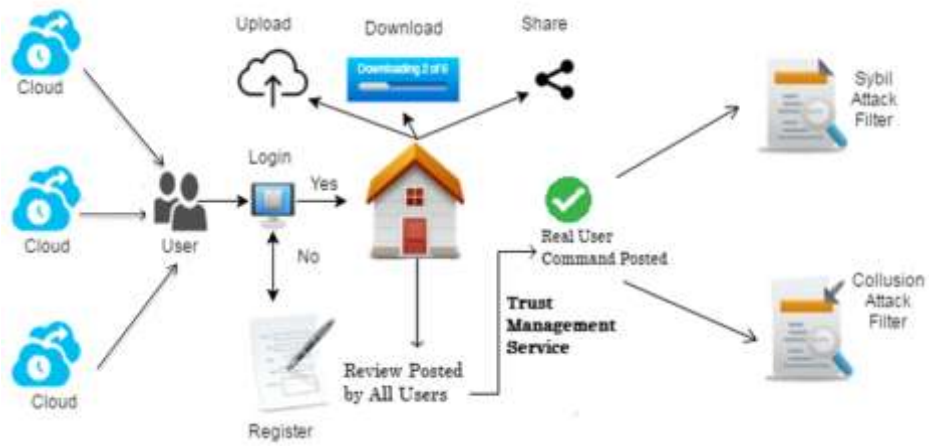
PROPOSED SYSTEM

We particularly focused on validating and studying the robustness of the proposed credibility model against different malicious behaviors, namely collusion and Sybil attacks under several behaviors, as well as the performance of our availability model. Our proposed credibility model is designed for i) the Feedback Collusion Detection including the feedback density and occasional feedback collusion, and ii) the Sybil Attacks Detection including the multi-identity recognition and occasional Sybil attacks. This means that our model can successfully detect collusion attacks (i.e., whether the attack is strategic such as in Waves and Uniform behavior models or occasional such as in the Peaks behavior model) and TMS is able to dilute the increased trust results from self-promoting attacks using the proposed credibility factors.

ADVANTAGES

1. The ability to detect strategic and occasional behaviors of collusion attacks.
2. The detection of such malicious behaviors poses several challenges.

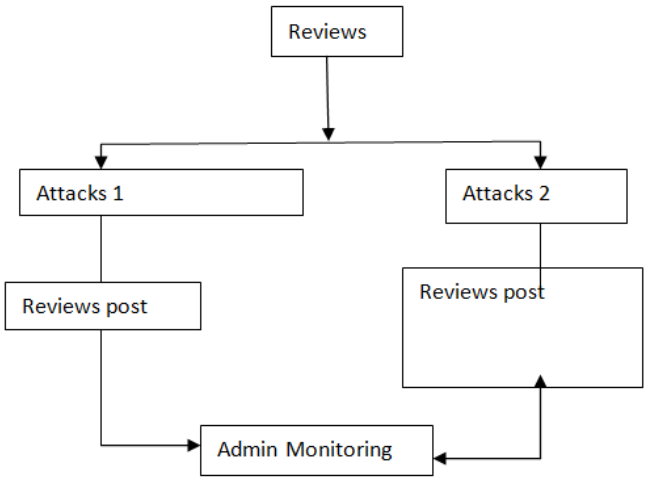
II. System Architecture



In this project threading concept is very important. A thread is a sequential path of code execution within a program. And each thread has its own local variables, program counter and lifetime. Like creation of a single thread, we can also create more than one thread (multithreads) in a program using class Thread or implementing interface Runnable to make our project efficient and dynamic. In our project we are using request process with the help of multi threading concepts.

SWINGS

Swing, which is an extension library to the AWT, includes new and improved components that enhance the look and functionality of GUIs. Swing can be used to build Standalone swing gui apps as well as Servlets and Applets. Employs a model/view design architecture. Swing is more portable and more flexible than AWT.



III. Modules

There are six modules in the project

1. **Advertisement**
2. **Cloud Selection and Registration**
3. **File Sharing**
4. **Posting Reviews**
5. **Filtering Reviews**
6. **Monitoring**

ADVERTISEMENT: The important role of the advertisement is to buy the best cloud. This module is created for security purpose. In this webpage we have to select any cloud provider. All cloud providers can upload, download and share document to the end users.

Fig 2.6.2.1: *Advertisement*

CLOUD SELECTION AND REGISTRATION: This module is used to select the best cloud providers based on reviews and provides large facility to the users. One cloud provides free storage for 500 MB and another cloud provides 800 MB means, so select either one or two is best. Then create a new account and register using user details.

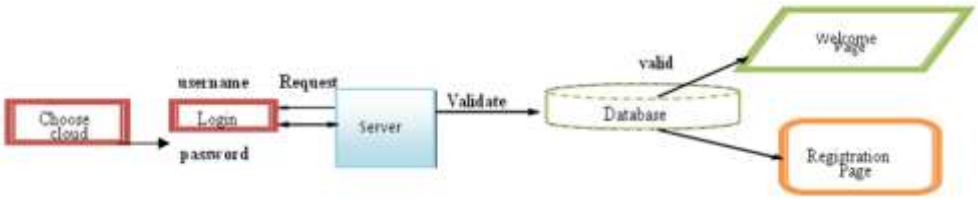


Fig 2.6.2.1: *Cloud Selection And Registration*

FILE SHARING: This module is used for sharing and uploads the files. It is easy to generate the all files and send it to the inter cloud users. It is easy to store and retrieves the data securely. And sends the files to all other users within a few seconds. So time is reduced compare with other clouds.

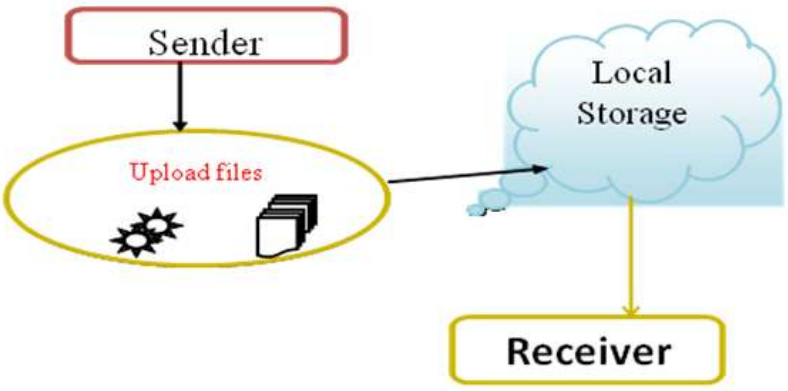


Fig 2.6.3.1: *File Sharing*

POSTING REVIEWS: In this module we give provide post on command all user in any clouds. So review means positive and negative all commands posted to the all clouds. So any customer new entering to choose any clouds based on the reviews. So review real user only provides that is good to the commands.

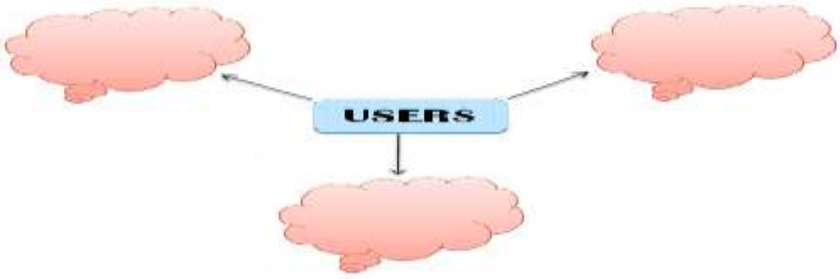


Fig 2.6.4.1: *Posting Reviews*

FILTERING REVIEWS: In this module summarization is important to we commands on only real user provides. Malicious users may give numerous fake feedbacks to manipulate trust results for cloud services (i.e., Self promoting and Slandering attacks). Some researchers suggest that the number of trusted feedbacks can help users to overcome such manipulation where the number of trusted feedbacks gives the evaluator a hint in determining the feedback credibility. However, the number of feedbacks is not enough in determining the credibility of trust feedbacks.

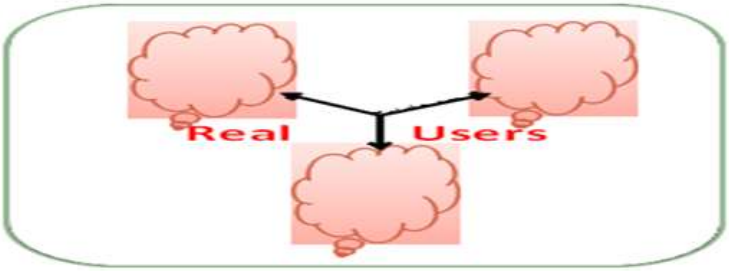


Fig 2.6.5.1: *Filtering Reviews*

MONITORING: In this module we attack find to collusion and Sybil attacks find easy. Also known as collusive malicious feedback behaviors, such attacks occur when several vicious users collaborate together to give numerous misleading feedbacks to increase the trust result of cloud services a self-promoting attack or to decrease the trust result of cloud services a slandering attack This type of malicious behavior can occur in a non-collusive way where a particular malicious user gives multiple misleading feedbacks to conduct a self-promoting attack or a slandering attack. Sybil Attacks Such an attack arises when malicious users exploit multiple. We assume a transaction-based feedback where all feedbacks are held in TMS to give numerous misleading feedbacks (e.g., producing a large number of transactions by creating multiple virtual machines for a short period of time to leave fake feedbacks) for a self-promoting or slandering attack.

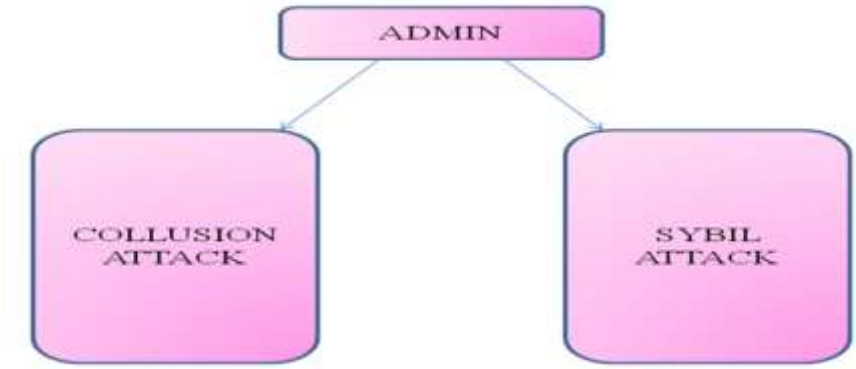


Fig 2.6.6.1: *Monitoring*

IV. Conclusion

Given the highly dynamic, distributed, and non transparent nature of cloud services, managing and establishing trust between cloud service users and cloud services remains a significant challenge. Cloud service users' feedback is a good source to assess the overall trustworthiness of cloud services. However, malicious users may collaborate together to i) disadvantage a cloud service by giving multiple misleading trust feedbacks (i.e., collusion attacks) or ii) trick users into trusting cloud services that are not trustworthy by creating several accounts and giving misleading trust feedbacks (i.e., Sybil attacks). In this paper, we have presented novel techniques that help in detecting reputation based attacks and allowing users to effectively identify trustworthy cloud services. In particular, we introduce a credibility model that not only identifies misleading trust feedbacks from collusion attacks but also detects Sybil attacks no matter these attacks take place in a long or short period of time (i.e., strategic or occasional attacks respectively).