JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Reliable Data-Sharing Responsibility Mechanism in the Cloud computing.

Akheel Mohammed*and Ayesha

Abstract

The term "cloud computing" refers to the practice of utilizing remote data centers and other computing facilities to complete tasks. It paves the way for highly scalable services to be consumed on-demand over the internet. One defining feature of cloud services is that customers' data is typically processed on unrecognizable devices outside of their control. While the convenience of this new technology is undeniable, users' concerns about privacy may prevent them from fully embracing cloud services. It has the potential to become a major barrier to widespread use of cloud services. We propose a highly decentralized answerability framework to monitor the actual utilization of users' data in the cloud, which would be a significant step toward solving this issue. In this paper, we present a cloud information accountability framework that uses automated logging and distributed auditing to keep track of who accessed what, when, and where in the cloud. We propose an object-oriented method that allows us to wrap the user's data and policies in the same container as our logging technique. The proposed solution would also deal with the JAR file, turning it into obfuscated code that will further fortify the system's defenses. In addition, we will be implementing a system of proved data possession for integrity verification, which will greatly improve the safety of users' data.

Keywords: Cloud Computing, Data Sharing, Information accountability framework, Provable data possession.

1. Introduction

The system for cloud information auditing presented in this study uses automatic logging and distributed auditing to keep track of who accessed what, when, and where in the cloud. A logger and a log harmonizer are its two primary parts. To define if and how cloud services and maybe other data stakeholders can access the

content, the JAR file provides a set of simple access control rules. Other than that, we'll make sure the JRE on the computers where the logger components are run is legitimate. While this new technology has many benefits, people are also starting to worry about giving up control of their personal data. Outsourcing the cloud's data processing raises responsibility concerns, especially when it comes to the protection of sensitive information like names and addresses. These concerns have emerged as a major roadblock to widespread use of cloud services. Oblivious hashing is used to perform these integrity checks. The proposed solution would also deal with the JAR file, turning it into obfuscated code that will further fortify the system's defenses. In addition, we will strengthen the safety of user information by using verifiable data holdings to ensure data integrity. The JAR will either provide use management in conjunction with logging, or it will provide solely logging functionality, depending on the configuration options defined at the time of creation. In terms of logging, the JAR will generate a log record whenever the data is accessed. Cloud computing, in the current system, is the distribution of computing as a service rather than a product, in which computers and other devices are provided with access to a common pool of hardware, software, and data via a network utility, analogous to how energy is distributed to homes and businesses. These days, a single server handles all of the user requests. Due to the server having to handle two requests at once, the total processing time is increased. As a result, data integrity issues, transaction delays, and compromised wallet data are all possible, and you can't put your trust in the underlying data infrastructure or service providers. While this new technology has many benefits, people are also starting to worry about giving up control of their personal data. Outsourcing the administration of sensitive data, such as that stored in the cloud, raises a number of accountability concerns. To put users' minds at ease, a reliable means for tracking how their data is being used in the cloud should be made available. For instance, due to the following characteristics of cloud environments, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign up for services, or approaches with a centralized server in distributed environment are not suitable.

Disadvantage: The database management system is not trustworthy in cloud computing, despite the fact that it is a rapidly expanding and improving technology.

A unique cloud-based automatic and legally binding logging technique is proposed. To the best of our knowledge, this is the first proposal of its kind, a systematic method for ensuring data accountability via the innovative use of JAR files.

This post is a follow-up to a conference paper we presented previously. The following are some of our recent improvements. To ensure the reliability of our system in the face of a corrupted JRE, we first incorporated integrity checks and an obvious hashing scheme. We have also improved the log records structure to give you more confidence in their honesty and legitimacy. We broaden the scope of the security analysis to include more types of attacks. We next detail the outcomes of further experiments and offer an in-depth analysis of the system's effectiveness.

2.Related Research

The first review of books and articles dealing with cloud computing privacy and security. We then briefly review other works that use methods analogous to our own, albeit for different ends.

2.1 Privacy and safety in the cloud

The idea behind them is that sensitive user information can be securely transmitted to the cloud and then processed there. The correct processing result is revealed after being deobfuscated by the privacy manager. However, the privacy manager has limited functionality in that it cannot ensure data security after it has been published. The authors' main focus is on leveraging trust connections for accountability in addition to authentication and anomaly detection, which is considerably different from our own. Most academic work on accountability has focused on how to make it a cryptographically proven quality, notably in the setting of online transactions. Crispo and ruffo put forth a novel theory on responsibility in delegation. Since we are not attempting to manage the cloud-based flow of data, delegation is a useful tool that complements our efforts. To the best of our knowledge, only the work by lee and colleagues proposes a decentralized method of establishing responsibility. The authors suggest a grid-centric agent-based system.

2.2 Related Methods

Our approaches' security is based on Java-based mechanisms for protecting self-defending objects. It is an extension of the object-oriented programming paradigm that software objects that provide sensitive functions or store sensitive data are tasked with defending themselves. Since the CIA system given in this study is based on similar architecture, we gave a java-based solution to the problem of privacy leaking during indexing. The proof carrying authentication framework was proposed by Appel and Felten. The PCA is concerned with web service access management and features a high order logic language that permits quantification over predicates. In addition, Mont et al.'s approach provides an identifying-based encryption method for access control. We use IBE methods as well, though in a very unique fashion. We do not count on IBE to enforce compliance between content and regulations. We utilize it to safeguard the encrypted data and the logs from threats like tampered plaintext and ciphertext attacks. While concerns about the safety of data storage are related to privacy, they are outside the scope of this work.

3. The Proposed system

To address these issues, we suggest a unique approach built on the concept of information

accountability: the Cloud Information Accountability framework. After data encryption, the data owner can then upload the data to the cloud server. Users can subscribe to the cloud server and be granted varying degrees of access to the original data (read, write, copy). The Loggers and Log Harmonizer will monitor and report on the data's access logs. In this paper, we offer a framework for ensuring the accountability of data stored in the cloud by automatically recording and auditing any relevant access made by any organization at any time. Both the Logger and the Log harmonizer are essential parts of it.

Benefit: we can exchange information in a safe and reliable environment.

3.1 Flow of Data

Each user starts by generating their own unique public and private Identifier-Based Encryption (IBE) keys. One of the most common attacks against our design is mitigated by this IBE scheme, which is a Weil pairing based IBE scheme. A logger component, in the form of a JAR file containing the necessary items, will be created by the user using the generated key.

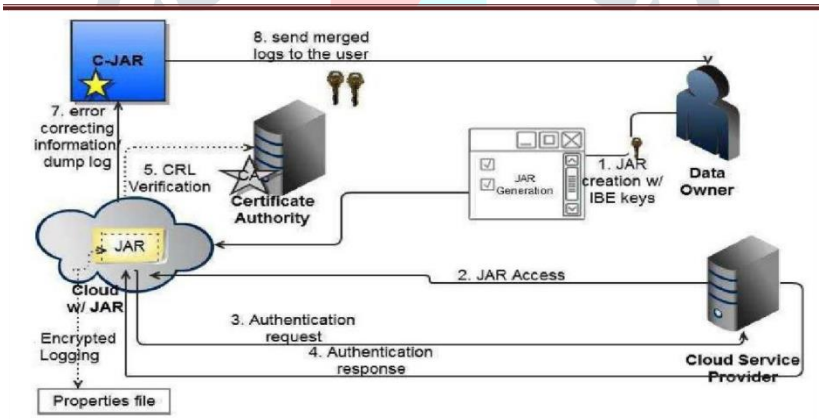


Figure 1. Overall Architecture.

Modification:

Each user's random numbers would be generated by the data owner, and any illegal actions would be reported automatically. When logging in, the user must enter the random number they generated, which will be checked by the server. If the verification is successful, then the user's account will be accessible only to them.

4.Implementation

4.1 The Development of the Suggested Algorithm

In this case, we employ a Log Retrieval Algorithm that operates in both Push and Pull modes. In the case of pure Log, the method shows logging and synchronization steps with the harmonizer. The algorithm initially determines if the JAR has grown too large or if the period between dumps has been longer than usual. At the time of JAR creation, the data owner defines the minimum and maximum allowable dump sizes and durations. The program can also tell if the data owner has asked for a dump of the logs. In the absence of any of these conditions, it will continue with the encryption of the record and the transmission of the mistake correction data to the harmonizer. A handshake is the first step in interacting with the harmonizer. When no reply is received, an error is recorded in the log file. When an issue occurs, the data owner is notified by email if the JAR is set up to do so. After the initial handshake is complete, a TCP/IP protocol is used to carry on the conversation with the harmonizer. If either of those things has happened, JAR simply deletes the log files and clears out all the variables so that a new record can be made. Verify that the CSP accessing the Access Log meets the requirements outlined in the relevant policies. If the requirements are met, permission is granted; otherwise, it is denied. The attempted access to the JAR file data will be noted regardless of the outcome of the access control. There are two primary benefits to our auditing system. To begin, it ensures a very high degree of log availability. Second, the harmonizer reduces the time it takes humans to examine massive amounts of data contained inside the log files that are transmitted by many versions of JAR files. Many kinds of modules, including but not limited to

4.1.1Owners/Users of the Data

The sailor/user is departing for sea/downloading data from the cloud server. A user must sign up with the cloud server in order to access the data stored there. Users will be required to sign up with information such as a username, password, and random numbers. For future authentication purposes, this data will be stored in a database. The owner of the data is the person responsible for storing it in the cloud. The Data Owner must sign up for a Cloud Server account before any data may be sent there. The space will be allocated to the Data Owner once they have enrolled on the cloud server.

4.1.2Hosted Web Server

The cloud server is where both the user and the data owner will store their information. To get the information you need, users must first submit a request to a cloud server, which will then relay the message to the data's rightful owner. The cloud server will also save user and data owner details in a database for later use.

4.1.3Logger

The Cloud Server is responsible for maintaining the log. The cloud server's loggers record information about the data's owner and any users who use the server. So, the Logger will serve many more functions. Including the identity of the data's rightful owner, the time and date of the request, and the IP address of the requesting user.

4.1.4Certifying Body

To ensure the Cloud server is legitimate, the certificate authority is consulted. The certificate authority must validate the cloud server. A fraudulent Cloud server is one that goes undetected by the user. The data owner can verify if the claims were true. Since the data owner will be storing their information in the cloud.

4.1.5 Authorized Access

Depending on the Owner, you may merely be able to read the content or even download it. Once the Cloud Server detects that a user has exceeded their permitted data access, they will send a dynamic warning. As a result, cloud data exchange is made much safer.

4.1.6 Concept of Push and Pull

The owner of the data may be able to see a list of everyone who accessed the file at a given moment. The cloud server will inquire during the signup process as to whether the data owner prefers the pull or push approach. With the pull technique, the data owner initiates contact with the cloud service provider to inquire about the current state of their data's accessibility.

4.1.7Generating Random Sets and Checking Them

The user must enter the random number set while making the data download request from the Cloud Server. If it's a good match, the user will be able to get their hands on the files. The pool of random numbers is changed each time. This safeguards the download of the data.

5.The End of the Experiment

Our system's performance is analyzed once we reveal the test environment conditions. The log harmonizer is stored in a separate location, either in a secure proxy or on the user end, making it inaccessible to the attacker and hence not considered in this attack. Therefore, we believe the log harmonizer is secure and the attacker

cannot access the decryption keys.

We begin our studies by measuring the overhead in the system and then analyzing the time it takes to generate a log file. Both when each individual log record is being encrypted and when all of the logs are being combined. In addition, JAR appears to be a file compressor for the files it manages. In particular, the suggested solution allows a single logger component to handle data for several files. We investigated whether using a single logger component to handle many files increased the size of the system.

5.1Time of Log Generation

In the first set of tests, we are interested in measuring how long it takes for a log file to be created when there are entities that are constantly accessing the data, which results in continuous logging. The outcomes are depicted in fig2. To be more precise, it takes on average 114.5 ms to produce a 100 Kb file, and 731 ms to develop a 1 MB file. Using the results of this experiment as a starting point, one can calculate the minimum interval between dumps while also taking into account factors like available storage space and network congestion.

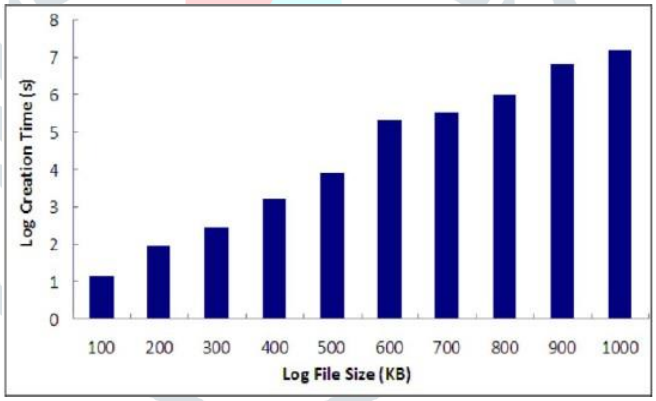


Fig .2. Time to merge log files.

5.2 Time of Authentication

Certificates can be cached to further boost performance. When only the JAR-required steps, such as obtaining a SAML certificate and then analyzing it, are taken into account, the time it takes to authenticate an end user is almost the same. This is done in a similar method by the JAR for both OpenSSL and SAML certificates. The average time for user activity is 1.2 minutes.

5.3 Effort Required for Logging Activities

The impact of log file size on logging performance is investigated in this set of experiments. We timed how long it took to allow an access and how long it took to write the accompanying log entry. Since every interaction is merely a view request, the time required to carry it out is quite small. In this way, the time it takes to record an event—whether it be the time it takes a user to double-click the JAR or the time it takes a server to run the script to open the JAR—is typically around 10 seconds. We also measured the time it took to encrypt the log, which was around 300 ms despite having no apparent correlation to the size of the file.

5.4 It Takes Logs to Merge

To determine if the log harmonizer is a bottleneck, we measured how long it took to combine log files. Here, we show that 10–25% of the records in the different log files are identical. Each each run of the experiment yielded a different average number of shared records. Ten repeats were used to calculate the average time. We timed how long it took to combine 70 log files ranging in size from 100 KB to 1 MB. Figure 3 displays the obtained outcomes. The time required to merge two 100 KB log files takes the least amount of time (59 ms) and increases practically linearly with the number of files and file size. When 70 files of 1 MB each were combined, the process took 2.35 minutes.

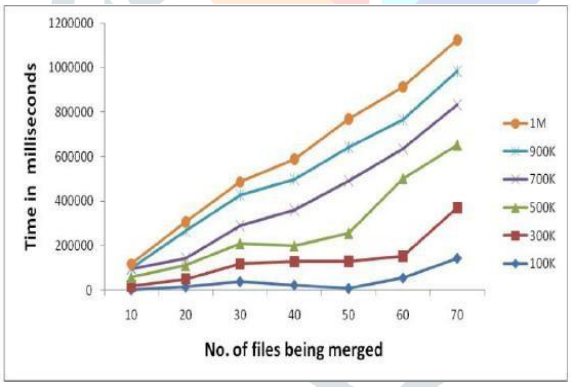


Fig.3. Time to create log files of different sizes.

When moving from 200 KB to 1 MB for content items, the logger size increases from 3525 to 4035 KB. Because of the compression offered by JAR files, the logger's overall size is determined by the largest files it stores. Please take note that we avoided including massive log files on purpose. In order to focus on the additional load that having numerous content files in a single JAR creates. The results are shown in Fig.4.

6 Conclusion

We implemented state-of-the-art methods, including an auditing tool, for automatically logging all cloud data access. With our method, the data owner can perform thorough content audits and, if necessary, implement robust back end protection. In addition, we have included PDP approach to improve the authenticity of owners' data. We hope to improve our method for ensuring JRE's authenticity in the future. To that end, we shall investigate whether or not the benefits of secure JVM being created can be utilized. By IBM, and we'd like to improve our PDP architecture from the end user's perspective so that data can be checked remotely and efficiently across several clouds.

References

1. Text Books

[1] Cloud Computing, Principles and Paradigms by John Wiley & Sons.

2. Conference Proceedings

1. Ensuring Distributed Accountability for Data Sharing in the Cloud Author, Smitha Sundareswaran, Anna C.Squicciarini, Member, IEEE, and Dan Lin, IEEE Transactions on Dependable and Secure Computing ,VOL 9,NO,4 July/August 2012 .
2. Hsio Ying Lin,Tzeng.W.G, **"**A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding ",IEEE transactions on parallel and distributed systems,2012.
3. Yan Zhu, Hongxin Hu, Gail Joon Ahn, Mengyang Yu, "Coopera-tive Provable Data Possession for Integrity Verification in Multi-Cloud Storage" , IEEE transactions on parallel and distributed systems,2012.

3. Generic Website

Network Traffic Classification Utilizing Machine Learning

UMME HANI SARA , Dr.B SASI KUMAR

M. Tech , Professor

Department of Computer Science and Engineering

DR.V.R.K. WOMEN COLLEGE OF ENGINEERING AND TECHNOLOGY

(Affiliated to JNTUH, Hyderabad,Approved by AICTE)

Hyderabad-500097

Telangana - India

Abstract-

In the world of networking, it sometimes becomes essential to know what types of applications flow through the network for performance of certain tasks. Network traffic classification sees its main usage among ISP's to analyze the characteristics required to design the network and hence affects the overall performance of a network. There are various techniques adopted to classify network protocols, such as port-based, pay-load based and Machine Learning based, all of them have their own pros and cons. Prominent nowadays is Machine Learning technique due to its vastness in usage in other fields and growing knowledge among researchers of its better accuracy among others when compared. In this paper, we compare two of the basic algorithms, Naïve Bayes and K nearest algorithm results when employed to networking data set extracted from live video feed using Wireshark software. For an implementation of Machine learning algorithm, python sklearn library is used with numpy and pandas library used as helper libraries. Finally, we observe that K nearest algorithm gives more accurate prediction than Naïve Bayes Algorithm, Decision Tree Algorithm and Support Vector Machine.

INTRODUCTION

As new technologies emerge, it has become more important to classify internet traffic (NTC). We investigate a wide variety of automated categorization methods.

Investigates how the efficiency of a blockchain application could influence the security of a mobile online loan. When an unauthorized network tries to utilize the channel, this feature might help identify it. This will help us learn more about its unique qualities. Knowing how to do this not only helps you spot foreign networks, but also the dangers that come from specific security holes in those networks. Maintaining network security and QoS is an important responsibility that may be accomplished via accurate techniques of characterizing networks. Depending on the level of compensation we feel appropriate, we have the right to limit or allow certain forms of traffic. Classifying networks improves productivity and revenue for broadcasters.

A multitude of network-based prediction models that can categorize various facets of online activity have emerged during the last several years. The terminal approach to traffic classification relied heavily on ports for many years. At first, everything went well. The data is analyzed by port to facilitate classification. Ports were registered with the International Issued Numbers Authority (IANA) for identification purposes. Not all of the links were functioning since they weren't listed on the Internet Assigned Number systems and hence couldn't use renumberable ports. We also talk about the many ways in which we might classify electronic communications. Then, the outcomes of several deep learning techniques are contrasted and compared. An original method for evaluating publication rankings was devised in this research by the authors, who used distributed denial-of-service (DDoS) assaults to disrupt target websites.

Payload-based methods are another option for discovering the kind of protocol a network packet uses. Since individual pieces of data are being inspected, this type of analysis of data is referred to as Deep The packet is Examination (DPE). Due to the high hardware implementation cost and subpar performance, this method is not useful for categorized packets. Despite these drawbacks, machine learning has seen widespread adoption due to its superior accuracy and resemblance to real-world data. In order to ensure accuracy, this method uses trained and tested models built from labeled classes.

In the following paragraphs, I'll talk about some of the specific contributions of this study. We next use machine learning methods to a dataset culled from the backbone of the internet and evaluate our ver

algorithms to see which is the most useful for evaluating traffic patterns. After being analyzed in Wireshark, the acquired characteristics are exported as.csv files so that they may be used to evaluate the effectiveness of the recommended use of Development tools for making predictions and doing additional comparisons.

Related work

Machine Learning for Traffic Classification on the Internet: a Literature Review

Methods for classifying network data that do not need the decoding the package bundles or the "well described" UDP or TCP control signals are gaining traction in the research community. Traffic data is increasingly being utilized as a part of the identification and categorization procedure. In order to categorize IP packets, more and more people are turning to Machine Learning (ML) techniques, which mix Infrastructural mode with data mining. Based on our review of 18 fundamental publications published between 2004 and the beginning of 2007, a time period during which techniques based on machine learning (ML) gained considerable attention, we provide the framework for future studies on Internet traffic categorization. Each piece of work is analyzed and rated based on the ML methods it employs and the relevance of the situations where it is applied. The reviewed works are scored by how well they conform to the specifications for ML-based protocol classification in enterprise-grade Internet protocols. Challenges and issues that have yet to be resolved are also covered.

Techniques based on machine learning to analyze and classify network traffic

The discipline of data science is now interested in studying how to classify Internet usage. There are many different kinds of network software, and ISPs need to be familiar with them all. The process of analyzing and categorizing mobile apps starts with the detection and labeling of online behavior. This method might be used to control the usual throughput. Port examination message evaluation, and device learning are just a few of the tried-and-true techniques that can be used to classify Internet traffic. In recent years, machine learning (ML) applications have become more popular. There are just too many studies showings that to be off by much. In this study, we use many distinct ml filters to classify network information. A congested collect tool is used to collect data on network bandwidth in real-time and a

feature based tool is then used to automatically extract that data. Some examples of these models are the C4.5 Decision Trees, the Naive Bayes Algorithm, the Bayes Net Classifier, and the Systematic Variable Model. The results of the experiments demonstrate the superiority of the C4.5 classifiers over their rivals.

Strategies for categorizing Internet traffic.

For a decentralized network to function, traffic classification is essential. Exposing the source of monitored communications has implications for Level of Service, online security, congestion visualization, and other areas. Due to the rise of P2P networking, packet forwarding has evolved significantly over the last decade. Researchers are always looking for new methods to better deal with the ever-changing Internet. There were a total of thirteen books, journals, and other publications produced on the subject of traffic categorization and associated issues between 2009 and 2012. We highlight the variety of current algorithms and provide recommendations on where conventional routing research should go next, including the significance of multi-level identification, the need of shared traffic data, and the relevance of model exploration.

METHODOLOGY

At times, it's vital to have insight into the kind of web-based tools and applications being used. Internet service providers often use congestion characterization and other indicators to assess the effectiveness of platform components used in network construction. Classification techniques based on things like ports, payloads, and computer vision are just a few examples. The advantages and disadvantages of each choice are different. Computer science has come to prominence on a worldwide scale as a result of its widespread use and the rising recognition among researchers of the better command it gives over earlier approaches. Using the Wireshark program, we analyzed the outcomes of two fundamental methods, the Nave Bayes method and the K closest approach, and gleaned link information from a movie stream or a network's packet capture. A machine learning method is constructed using the learning framework in Python, in addition to the NumPy and pandas' libraries. Finally, we see that the K nearest approach yields more in-depth forecasts than a Naive Bayes Algorithms the Decision Tree Algorithm, and the Support Vector Machine.

Current Infrastructure

Numerous network analyzers, each with the capacity to accurately categorize online behavior, have emerged during the last several decades. Messages have traditionally been organized using a method called "streaming," which relied on ports to differentiate between different networks. At first, everything went well. Port-based data analysis is used. The International Assigned Numbers Organization (IANA) was initially helpful in the categorization of ports. Most of the port aren't included in the IANA, which stands databases, thus they can't be renumbered, which caused the system to malfunction.

The suggestive system

We apply human learning techniques to a network data frame, then evaluate a large number of algorithms to determine which is most effective for studying web-based habits. Using Development tools, we first gather the data through a VLAN, then convert it to a file format and use it to train the classifier, then use the data to aid in predicting and do a comparison analysis. The company employs a wide range of decision-making approaches, including as DT, NB, KNN, which are etc., and SVM. KNN technique is better in this case.

Modules:

As part of the above project's execution, the following modules were developed:

Dataset of Network Traffic, Please Upload:

Put the following information online and connect to the internet:

Using these modules, they will provide data to the computer.

Prepare Your Data:

So that we can get rid of blanks and utilize ML methods that don't rely on character values, we convert the semi-languages to numbers and give each duplicated string an algebraic identifier. After the data has been thoroughly cleaned, it will be separated into test and training information, with the former making up 80% of the entirety and the latter 20%.

The KNN and Naive Bayes algorithms should be executed.

In this section, we convert the semi-languages to numbers and give each duplicate string an algebraic identifier to facilitate the removal of blanks and the use of ML methods that do not rely on character values. After the data sample has been

disinfected it will be split into test and training information, with the former making up 80% of its entirety and the latter 20%.

Conduct a Decision Tree Analysis.

The proposed method will be trained using a dataset that was used for predicting vehicle classification and evaluating the accuracy of the correct projection on test data.

Results and Discussion

Given the prevalence of non-numerical datasets, it is important to create a chart in which the x-axis indicates the type of network in question and the y-axis indicates the number of entries in the image database for that organization. Select "Data Preprocessing" to cancel the current graph and restart sampling."

SVM was applied to the same data as the previous screen, and 74% accuracy was achieved. If you hit the 'Run SVM Algorithm' button, you'll see the results below:.

SVM gave us a 50% success rate on the previous screen. Select "Comparison Graph" to get a tabular presentation of comparisons.

In terms of both x (the name of the algorithm) and y (the degree of accuracy

achieved), KNN is obviously superior than any other methods.

CONCLUSION

This research seeks to shed light on Ml Algorithm for dividing broadband traffic data by investigating many methods for identifying network events. If you're just starting out in data analysis, this study will help you choose which neural networks model is optimal for your use case. Roadway cleaning is performed in the first phase to test out the ML methods that will be presented in the second phase. In addition to networking and employee involvement, pattern recognition algorithms are also utilized in the categorization of unknown applications.

Next, we use artificial intelligence to delve into the foundational steps. This kind of network traffic data will be used to test and compare various Machine Learning-based classifiers. When comparing KNN to the Nave Bayes and the decision-tree algorithms, and the Supported Vector Algorithm in terms of reliability, KNN is clearly the winner. Reason being, compared to the Nave Bayes model and the dt, KNN is more flexible in terms of adopting a good limit. When compared to SVM and DT and NB, KNN was the most reliable. Furthermore, the most exacting requirements of precision are not infeasible to maintain.

REFERENCE

[1] Nguyen, Thuy TT, and Grenville Armitage. "A survey of techniques for internet traffic classification using machine learning." IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 56-76, 2008.

[2] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, and F. Abdessamia, “Network traffic classification techniques and comparative analysis using machine learning algorithms,” in Proc. IEEE International Conference on Computer and Communications (ICCC-2016), pp. 2451-2455, 2016.

[3] Internet Assigned Numbers Authority (lANA), http://www.iana.orglassignments/port-numbers, as of August 12, 2008.

[4] Pawel Foremski, “On different ways to classify Internet traffic: a short review of selected publications Theoretical and Applied Informatics,” 2013.

[5] K. Sing and S. Agrawal, “Comparative Analyssis of Five Machine Learning Algorithms for IP Traffic Classificat in

Proc. IEEE International Conference on Emerging Trends in Network and Computer Communication (ETNCC-2011), pp. 33-38, 2011.

[6] Q. Dai, C. Zhang and H. Wu, “Research of Decision Tree Classification Algorithm in Data Mining,” International Journal of Database Theory and Application, vol. 9, no.5, pp. 1-8, 2016.

[7] Cristina Petri, “Decision Trees”, Cluj Napoca, 2010.

[8] S. Karthika and N. Sairam, “A Naïve Bayesian Classifier for Educational Qualification,” Indian Journal of Science and Technology, vol. 8, no. 16, Jul. 2015; DOI: 10.17485/ijst/2015/v8i16/62055.

[9] D. K. Srivastava and L. Bhambhu, “Data Classification Using Support Vector Machine,” Journal of Theoretical and Applied Information Technology, vol. 12, no. 1, Feb. 2010.

[10] Wireshark tool: https://www.wireshark.org/docs/dfref/.

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Keyword Search and Dual-Server Public-Key Encryption for Secure Cloud Storage

Asmayeen*1, Dr. B. Sasi Kumar*2

*1 M.Tech Student- CSE, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

*2 Principal & Professor, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

Article Info
Volume 9, Issue 5
Page Number : 217-223

Publication Issue :
September-October-2022

Article History
Accepted : 10 Oct 2022
Published: 30 Oct 2022

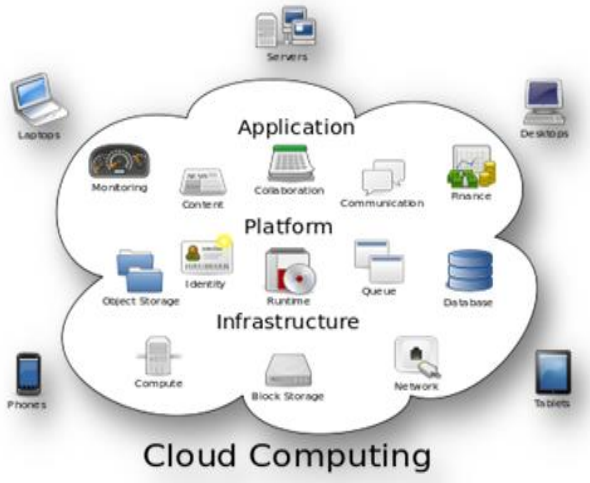
ABSTRACT

A growing number of people are interested in searchable encryption to safeguard the privacy of their data in secure searchable cloud storage. In this research, we examine the security of public key encryption with keyword search (PEKS), a widely used cryptographic fundamental with several applications in cloud storage. Unfortunately, it has been established that the conventional PEKS architecture has a flaw known as an inside keyword guessing attack (KGA) that is perpetrated by a rogue server. We suggest the dual-server PEKS framework as a new PEKS framework to remedy this security flaw (DS-PEKS). One further significant addition is the definition of a new type of smooth projective hash function (SPHF) called a linear and homomorphic SPHF (LH-SPHF). Then, using LH-SPHF, we demonstrate a generic construction of secure DS-PEKS. We propose an effective instantiation of the general framework from a Decision Diffie-Hellman-based LH-SPHF and demonstrate that it can accomplish the strong security inside the KGA to demonstrate the viability of our new framework.

Indexed Terms : Location-Based Social Network, Text Mining, Travel Route Recommendation

I. INTRODUCTION

Cloud computing (equipment and software) is used and shared remotely over a network in what is known as "the cloud" (usually the Internet). In structure graphs, a cloud-shaped picture is commonly used to represent the complex information it contains, hence the name. Through distributed processing, a client's information, code, and estimation can be shared amongst multiple, geographically dispersed organizations. System hardware and software for appropriate processing are available online from supervised pariah groups. Modern programming languages and server PC networks are made possible by these establishments.



Structure of cloud computing

Explaining the Workings of Cloud Computing.

Traditional supercomputing, or peak execution handling power, is typically reserved for use by the military and assessment agencies. The purpose of distributed registration is to put this type of processing power to use in client-centric applications, such as financial portfolios, the transmission of updated information, the provision of data limits, and the management of massive, visually impressive PC games. Distributed processing makes use of networks of very large groups of servers, which typically run low-cost client PC development and have some connection to dispersing data-handling tasks. Common IT architectures feature massive aggregations of interconnected systems. Virtualization methods are commonly used to increase the efficiency of distributed computing. Characteristics and Service Types: With the NIST's definitions in mind, here are some of the most remarkable aspects of widely disseminated numbers:

- Self-organization on demand: customer can set their limits for things like server time and association storage as needed, without needing to coordinate with each specialist facility individually.
- Capabilities are accessible over the network and can be used by a variety of client types thanks to standardized frameworks (e.g., cells, PCs, and PDAs).
- Resource pooling: In a multi-tenant model, the provider shares its enlisting resources among its many clients, allocating and reallocating its physical and digital assets to each client by their needs. Since the client generally has no control or data over the specific region of the provided resources at this point, there is a sense of region opportunity and the client may have the option to decide region at a higher level of reflection (e.g., country, state, or server ranch). Resource situations consist of constraints, management, memory, data transmission over networks, and virtual machines.
- Rapid adaptability: Capabilities can be provisioned quickly and skillfully, occasionally normally, to rapidly scale out, and immediately conveyed to rapidly scale in. Often, the client has the impression that they can purchase an unlimited amount of provisioning at any time.
- A metering limit appropriate to the type of business is typically used by cloud architectures to manage and expand resource utilization (e.g., limit, dealing with, information transmission, and dynamic client accounts). Both the user and the resource provider can benefit from due, controlled, and definitive resource use.

Characteristics of cloud computing

II. RELATED WORK

1) A new generic framework with a keyword search for safe public key encryption

R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang are the authors.

Users can search encrypted files on an untrusted server using Public Key Encryption with Keyword Search (PEKS), a technology developed by Boneh et al. in Eurocrypt'04. The cryptography research community has paid a lot of attention to this idea because it has many practical uses. All of the current PEKS schemes, however, have the drawback of being unable to withstand the Keyword Guessing Attack (KGA) initiated by a hostile server. In this research, we present Dual-Server Public Key Encryption with Keyword Search as a new PEKS architecture (DS-PEKS). As long as the two untrusted servers do not cooperate, this new structure can withstand every assault, including the KGA. Then, using a fresh iteration of the Smooth Projective Hash Functions (SPHFs), we propose a general construction of DS-PEKS that is also of interest.

2) Improved definitions and effective structures for searchable symmetric encryption

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky are the authors.

A party can delegate the private storage of his data to a third party while still having the option to conduct limited searches on it thanks to searchable symmetric encryption (SSE). Research on this issue has been ongoing, and several security definitions and constructions have been put out. In this essay, we first examine current security concepts before putting forth new, more robust security definitions. Then, we provide two constructions that, according to our new definitions, are secure. Interestingly, our buildings are more effective than any preceding constructions and also satisfy better security assurances.

Additionally, earlier research on SSE only took into account the scenario in which only the owner of the data can submit search queries. We take into account the logical extension where search queries can be submitted by any arbitrary group of parties aside from the owner. In this multi-user environment, we explicitly define SSE and propose an effective construction.

3) K-Resilient IBE-based Public Key Encryption with Keyword Search

TITLE: D. Khader

Abstract. Bob sends Alice an email that has been encrypted. For some reason, a gateway needs to see if a specific keyword is present in an email or not (e.g. routing). However, Alice does not want anybody else, not even the gateway, to be able to decode the email. This situation calls for the use of public key encryption with keyword search (PEKS). In this study, we develop the KResilient Public Key Encryption with Keyword Search (KR-PEKS), a novel technique. Without the random oracle, the new technique is secure against a chosen keyword attack. The

The KR-PEKS was created using the capability of creating a Public Key Encryption with Keyword Search from an Identity Based Encryption. By demonstrating that the used IBE had a notion of key privacy, the security of the proposed system was demonstrated. The system was then changed in two distinct ways to achieve each of the following: the first change enabled multiple keyword searches, and the second change did away with the requirement for secure channels.

4) Generic secure-channel encryption that is open to search and has adaptive security

K. Emura, A. Miyaji, M. S. Rahman, and K. Omote are the authors.

A public key encryption system with keyword search (PEKS) and its variant secure-channel free PEKS (SCF-PEKS) have been proposed for keyword searches against encrypted material. In this research, we expand the security of SCF-PEKS and provide adaptive SCF-PEKS, where an adversary is allowed to issue test queries adaptively (modeled as a "malicious but legitimate" receiver). We demonstrate that only anonymous identity-based encryption is capable of

generically constructing adaptive SCF-PEKS. In contrast to the PEKS construction by Abdalla et al. (2008), SCF-PEKS can be created without the need for any additional cryptographic primitives, even though adaptive SCF-PEKS necessitates additional capabilities.

We also provide an alternative adaptive SCF-PEKS structure that is more effective than the previous one while not being entirely generic. In comparison to the (non-adaptive secure) SCF-PEKS scheme by Fang et al., we finally instantiate an adaptive SCF-PEKS scheme (using our second construction) that achieves a similar degree of efficiency for the costs of the test procedure and encryption (CANS2009). 2014 John Wiley & Sons, Ltd. Copyright 5) Cooperative data possession for multi-cloud storage integrity verification

5) Offline keyword guessing attacks using keyword search techniques on modern public key encryption W.-C. Yau, S.-H. Heng, and B.-M. Goi is the author.

Boneh et al. introduced the Public Key Encryption with Keyword Search Scheme (PEKS) for the first time in 2004. The issue of searching through material that has been encrypted with a public key setting is resolved by this scheme. The Secure Channel Free Public Key Encryption with Keyword Search (SCF-PEKS) technique, which eliminates the secure channel for sending trapdoors, was recently suggested by Baek et al. Later on, they put out the PKE/PEKS system, an upgraded PEKS method that incorporates a PKE scheme. We discuss offline keyword guessing attacks against SCF-PEKS and PKE/PEKS methods in this work. We show that offline keyword guessing attacks allow external adversaries who intercept trapdoors sent over a public channel to decrypt encrypted keywords. While internal enemies can carry out assaults regardless of whether trapdoors are supplied over a secure or public channel.

III. SYSTEM ANALYSIS

Existing System

- In a PEKS system, the sender encrypts some keywords (called PEKS ciphertexts) with the receiver's public key and appends them to the encrypted data. The receiver then communicates with the server with the backdoor of a search term. The server can determine if the keyword used by the receiver in the PEKS ciphertext is the same as the one used in the trapdoor by comparing the two. If it does, the server will give the recipient the appropriate encrypted information. A new PEKS strategy, called a secure channel-free PEKS, was proposed by Baek et al., which eliminates the need for a secure channel (SCF-PEKS).
- Security for SCF-PEKS was improved by Rhee et al. after it was discovered that an attacker may learn about the connection between the non-challenge ciphertexts and the trapdoor.
- Since users typically employ well-known terms when looking for documents, Byun et al. introduced the offline keyword guessing attack against PEKS.

CONS: The current system has many drawbacks.

- Despite not requiring the dissemination of secret keys, PEKS methods are not completely secure due to a vulnerability in the trapdoor keyword privacy, more specifically the Keyword Guessing Attack (KGA). Security is compromised because anyone with knowledge of the receiver's public key can produce the PEKS ciphertext of any random keyword.
- To be more precise, an adversarial server equipped with a trapdoor can select a guessing term from the keyword space and use it to produce a PEKS ciphertext. When a guess is made, the server can see if it matches the secret keyword. Repeating

this process of guessing and testing until the right keyword is identified is possible.

- One problem is that the server does not have a hard time determining which small set the underlying keyword is a part of, even if it cannot guess the keyword itself. This means that the keyword's privacy is not properly safeguarded from the server. However, their plan is infeasible since the recipient must independently locate the correct ciphertext by utilizing the exact trapdoor to eliminate all but the one correct answer from the set supplied by the server.

THE SUGGESTED SYSTEM:

This study makes four major contributions.

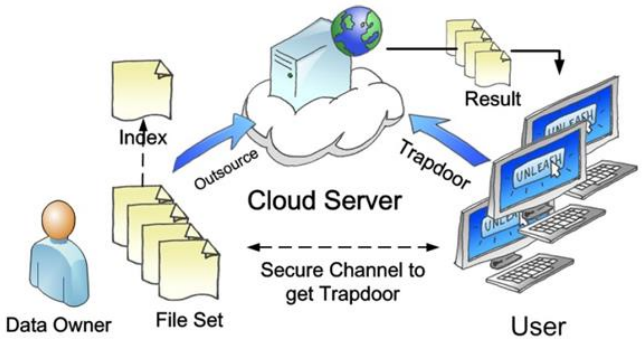
- To fix this security hole in PEKS, we create a new framework we call Dual-Server Public Key Encryption with Keyword Search (DS-PEKS).
- For a more general DS-PEKS design, we present a linear and homomorphic form of the Smooth Projective Hash Function (SPHF) called linear SPHF.
- Using the proposed Lin-Hom SPHF, we demonstrate a generic construction of DS-PEKS.
- In this study, we describe a practical implementation of our SPHF based on the Diffie-Hellman language to demonstrate the viability of our novel framework.

PROPOSED SYSTEM BENEFITS

- Since our technique does not require any pairing computation, it is more efficient than existing systems that do require pairing computation during the production of PEKS ciphertext and testing.
- It has been determined that our method achieves the highest PEKS computation efficiency. The reason is, our plan leaves out the computation of pairs deliberately. In particular, the current technology has the highest calculation cost because each generation of PEKS requires 2 pairing computations.
- We do not need to perform any pairing computation, and the server takes care of all the searching, so our scheme has a lower computation cost than any existing scheme, despite requiring an additional step for the testing.

IV. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE:



MODULES:

- Module for Building Systems
- Security against Selective Keyword Semantics
- Server at the Front
- Back Server

CONTENTS OF MODULES:

Module for Building Systems

Our first module focuses on building the foundation of our system by creating the necessary data structures and entities. 1) Cloud User: the person or business who initially placed data in the cloud and is now using that data. 2) CSP: cloud service provider, the company in charge of running CSS and selling access to their network's cloud storage space to customers. We introduce the formal concept and security models of the new framework we propose, called DS-PEKS. Later, a new type of smooth projective hash function is defined by us (SPHF). Formal correctness analysis and security proofs are presented to demonstrate a general construction of DS-PEKS from LH-SPHF. In

conclusion, we show that SPHF can be used to efficiently implement DS-PEKS.

Security against Selective Keyword Semantics

To ensure that an attacker cannot tell one keyword apart from another when presented with a PEKS ciphertext, we implement semantic security against a chosen keyword attack in this section. In other words, an opponent cannot deduce the underlying keyword from the PEKS ciphertext.

Server at the Front

When the front server receives a query from the receiver, it uses its private key to pre-process the trapdoor and all the PEKS ciphertexts. It then provides the rear server with a set of testing states that conceal the relevant trapdoor and PEKS ciphertexts.

Back Server

Using its private key and the obtained internal testing states from the front server, the back server can then decide which documents are queried by the receiver in this section.

III. CONCLUSION

In this research, we propose a novel framework called Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to address a flaw in the standard PEKS architecture: the possibility of an inside keyword guessing attack. In addition, we developed a new Smooth Projective Hash Function (SPHF) and applied it to the creation of a generalized DS-PEKS protocol. The research also presents a practical implementation of the new SPHF based on the Diffie-Hellman issue, which yields a practical DS-PEKS method without pairings.

IV. FUTURE WORK

In the Future, Long-Term Impact: In MessageLocked Encryption (MLE), a new cryptographic primitive, the key used to encrypt and decode the message is itself obtained from the message. Numerous cloud-storage companies aim to provide secure deduplication (space-efficient secure outsourced storage), and MLE gives the means to do so. It defines confidentiality as well as a type of integrity known as tag consistency.

V. REFERENCES

[1]. R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, "A new general framework for secure public key encryption with keyword search," in Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP), 2015, pp. 59–76.

[2]. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44–55.

[3]. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[4]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), 2006, pp. 79–88.

[5]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Int. Conf. EUROCRYPT, 2004, pp. 506–522.

[6]. R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in Proc. Int. Conf. EUROCRYPT, 2003, pp. 524–543.

[7]. B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in Proc. NDSS, 2004, pp. 1–11.

[8]. M. Abdalla et al., "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in Proc. 25th Annu. Int. Conf. CRYPTO, 2005, pp. 205–222.

[9]. D. Khader, "Public key encryption with keyword search based on K-resilient IBE," In

Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2006, pp. 298–308.

[10]. P. Xu, H. Jin, Q. Wu, and W. Wang, “Publickey encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack,” IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

Cite this article as :

Asmayeen, Dr. B. Sasi Kumar, "Keyword Search and Dual-Server Public-Key Encryption for Secure Cloud Storage", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 217-223, September-October 2022.
Journal URL : https://ijsrset.com/IJSRSET229536

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Cold-Start Product Recommendation Using Microblogging Information: Linking Social Media To E-Commerce

G. Roja[*1], Dr. B. Sasi Kumar[*2]

[*1] M.Tech Student- CSE, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

[*2] Principal & Professor, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

Article Info
Volume 9, Issue 5
Page Number : 224-228

Publication Issue :
September-October-2022

Article History
Accepted : 10 Oct 2022
Published: 30 Oct 2022

ABSTRACT

The lines between online shopping and social networking have blurred in recent years. Social login allows users to access their favourite e-commerce sites by logging in with credentials from their existing account on a third-party social network like Facebook or Twitter. Additionally, customers can promote their recent purchases on microblogs by including links to the item pages on the merchant's website. To recommend products from e-commerce websites to users on social networking sites in "cold-start" situations, this paper proposes a novel approach to the under-explored problem of cross-site cold-start product recommendation. The challenge of figuring out how to use knowledge extracted from social networking sites is a major one in implementing cross-site cold-start product recommendations. To facilitate the mapping of social networking features to another feature representation for a product recommendation, we propose using users who have accounts on both social networking sites and e-commerce sites as a bridge. To be more specific, we propose using recurrent neural networks to learn feature representations for users and products (termed user embedding's and product embedding's, respectively) from data collected from e-commerce websites, and then employing a modified gradient boosting trees method to transform users' social networking features into user embedding's. After acquiring user embedding's, we develop a feature-based matrix factorization approach to cold-start product recommendations. Experimental results on a large dataset constructed from SINA WEIBO, the largest Chinese microblogging service, and JINGDONG, the largest Chinese B2C e-commerce website, confirmed the efficacy of our proposed framework.

Keywords : Online Store , Online Business I, Jingdong, Sina Weibo

I. INTRODUCTION

The lines between online shopping and social networking have blurred in recent years. Social network features, such as instantaneous updates and interactions between users, can be found on e-commerce sites like eBay. Social login is a feature

offered by some online stores that enable new customers to register with their existing credentials from a social media platform like Facebook, Twitter, or Google+. A "buy" button, accessible via advertisements or other posts, was introduced on both Facebook and Twitter in the past year, allowing users to make purchases without leaving the sites. Strategically investing in SINA WEIBO1 allows e-commerce giant ALIBABA to reach Chinese internet users with product advertisements. Data extracted from social sites is crucial especially in light of the growing popularity of using these platforms for e-commerce.

In this paper, we investigate the intriguing challenge of making product recommendations from e-commerce sites to social networking site users in "cold-start" situations, where no previous purchase data exists.

We referred to this issue as "cold start" product recommendations across multiple sites. Even though online product recommendation has been studied extensively, most studies only concentrate on building solutions within specific e-commerce websites and primarily use users' historical transaction records. Cross-site cold-start product recommendation appears to be an underexplored area. Because of the nature of the problem we're trying to solve, we're limited to using the users' social networking information to make recommendations.

To overcome this difficulty, we propose connecting users' social networking features to latent features for product recommendation through the shared users between social networking sites and e-commerce websites. To be more precise, we propose using recurrent neural networks to learn feature representations (called user embedding's and product embedding's, respectively). After learning user embedding's, we create a feature-based matrix factorization method to use for cold-start product recommendations.

II. RELATED WORK

Possibility-based framework for advising on online purchases: Just the right product, at just the right time:

The primary goal of most current e-commerce recommender systems is to match a user with a product they are more than likely to buy and enjoy. However, the timing of a recommendation can have a significant impact on its success. Take the brand-new laptop owner as an example.

If the laptop's original battery tends to stop holding a charge around the two-year mark, she may buy a replacement battery at that time and then a new laptop at the end of the four-year mark. In this case, it would be inappropriate to suggest that the user buy a new laptop or a replacement battery so soon after making the initial purchase. Getting the right product recommendation at the wrong time can lower the user's opinion of the recommender system.

While it's important for a system to recommend the most applicable item, we argue that it's also important for it to recommend at the optimal time.

The paper investigates the contemporary issue of making timely product suggestions. Here, we apply the proportional hazards modelling strategy from survival analysis to the study of recommendations and propose a new opportunity model for including time in an online store's individualized product recommendations.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM:

- Studies typically only look at specific e-commerce sites, and even then, they only look at solutions built with users' past transaction data. Cross-site cold-start product recommendation appears to be an underexplored area.
- The cold-start recommendation problem is also the subject of a substantial body of literature.
- In order to predict ratings for new users, Seroussi et al. proposed incorporating data from users' public profiles..
- The ensemble learning algorithm proposed by Zhang et al.
- Schein suggested a technique that would incorporate content and collaborative data into a unified probabilistic model.
- Using social data, Lin et al. solved the "cold-start" problem for app recommendations.

3.1.1 Disadvantages of the Current System

- Our cross-site cold-start product recommendation task is different from theirs in that they only consider the brand or category-level purchase preference based on a trained classifier.
- In contrast to the wide variety of features we investigated, they only consider gender, age, and Facebook likes.
- In order to solve the cross-site cold-start recommendation problem, they neglect to think about how to convert the varied data collected on social media platforms into a format suitable for use in online stores.

3.2 PROPOSED SYSTEM

- In this paper, we investigate the intriguing issue of making product recommendations from e-commerce sites to social networking site users in "cold-start" situations, where no previous purchase data exists. We referred to this issue as "cold start" product recommendations across multiple sites.
- Because of the nature of the problem we're trying to solve, we're limited to using the users' social networking information to make recommendations. To overcome this difficulty, we propose connecting users' social networking features to latent features for product recommendation using the shared user base of social media and online stores (users who have social networking accounts and have made purchases on e-commerce websites).
- We specifically propose using recurrent neural networks to learn feature representations for users and products (termed user embedding's and product embedding's, respectively) from data collected from e-commerce websites, and then using a modified gradient boosting trees method to transform users' social networking features into user embedding's.
- Next, we use the user embedding's we've learned to power cold-start product recommendations using a matrix factorization method based on feature engineering.

3.2.1 BENEFITS OF THE SUGGESTED SYSTEM:

- The cross-site cold-start product recommendation problem can be solved using our proposed framework.
- We expect our study to have far-reaching consequences for academic and commercial settings alike.

IV. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

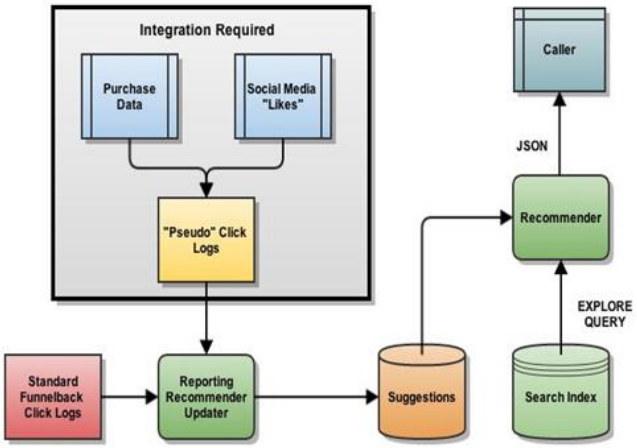


Fig: 4.1 system architecture

V. RESULT

The study states that social media and e-commerce are interconnected by each other.by using embedded system and microblogging system we can provide the user of both social media and e-commerce facilities in the same application. Also it helps the sellers to improves their business by recommending the required product for the user by data mining techniques. It collects user's data at the time of login and based on the data it provides recommendation of the required product and also Which increase the business we use peer to peer network for this particular paper. So but the limitation is we can only add the products and can review the product. almost customers purchase the product based on the previous reviews.so here we can provide the reviews as well.

We are certain that our view point towards the issue can be an impactful change in how consumers use

recommendations to shop online. We hope that this can reform how people use their social media to look for products that fit their requirements and also help e-commerce websites to reach their target audience with the right recommendation. This outlook is only a basic proposed solution; furthermore many effective-advance methods such as Convolutional Neural Network13 can be implied for feature learning.

VI. CONCLUSION

In this project, we investigate a new challenge: how to recommend products from e-commerce sites to microblogging users who don't have any purchase history. Our central thesis is that, through feature learning using recurrent neural networks, e-commerce website users and products can share a common latent feature space. Users who have accounts on both e-commerce and social networking sites can be used as a bridge to learning feature mapping functions by employing a modified gradient boosting trees approach. This approach maps users' attributes extracted from social networking sites onto feature representations learned from e-commerce sites.

Incorporating the mapped user features into a feature-based matrix factorization approach for cold-start product recommendation is a powerful strategy.
Using WEIBO and JINGDONG, we have assembled a sizable dataset. Our findings validate the efficacy of our proposed framework in solving the cross-site cold-start product recommendation issue. We anticipate significant repercussions from our study for academia and business alike.To learn user and product embedding's, traditional methods have only used a basic neutral network architecture. We can look into more cutting-edge deep learning models for feature learning in the future, like Convolutional Neural Networks13. In addition, we'll think about how to enhance the current feature mapping technique by transferring learning ideas.

VII. FUTURE WORK

Additional deep learning models, such as Convolutional Neural Networks13, can be investigated for feature learning in the future. We will also think about how to enhance the current feature mapping method using concepts from transfer learning. Learned user and product embedding's have previously only been implemented using a basic neutral network architecture. It is possible to improve the solution by attempting to identify more qualified traits from the client's online networking about the client, which will aid in the appropriate evaluation of the client's interest. Existing solutions may be integrated with it, such as linked product recommendation, which suggests complementary items to those already in a customer's inventory.

VIII. REFERENCES

[1]. Wang, C.; Zhang, P. The evolution of social commerce: The people, management, technology, and information dimensions.
[2]. Commun. Inf. Syst. 2012, 31, 105–127.
[3]. Han, H.; Xu, H.; Chen, H. Social commerce: A systematic review and data synthesis. Electron. Commer. Res. Appl. 2018, 30, 38–50.
[4]. Lin, X.; Li, Y.; Wang, X. Social commerce research: Definition, research themes and the trends. Int. J. Inf. Manag. 2017, 37, 190–201.
[5]. Busalim, A.H. Understanding social commerce: A systematic literature review and directions for further research. Int. J. Inf. Manag. 2016, 36, 1075–1088.
[6]. Statista. Revenue from Enterprise Social Networks Worldwide from 2010 to 2021 (in Million U.S. Dollars). 2015. Available online: https://www.statista.com/statistics/503514/worldwide-enterprise-social-networks-revenue/ (accessed on 7 December 2021).
[7]. Rubenstein-Montano, B.; Liebowitz, J.; Buchwalter, J.; McCaw, D.; Newman, B.; Rebeck,

K.; Team, T.K. A systems thinking framework for knowledge management. Decis. Support Syst. 2001, 31, 5–16.

[8]. Kitchenham, B. Procedures for Performing Systematic Reviews; Keele University: Keele, UK, 2004; Volume 33, pp. 1–26.

[9]. Kitchenham, B. Guidelines for Performing Systematic Literature Reviews in Software Engineering; Technical Report No. 2.3; IEEE: London, UK, 2007; pp. 1–65.

[10]. Liang, T.P.; Ho, Y.T.; Li, Y.W.; Turban, E. What Drives Social Commerce: The Role of Social Support and Relationship Quality.

Cite this article as :

G. Roja, Dr. B. Sasi Kumar, "Cold-Start Product Recommendation Using Microblogging Information: Linking Social Media To E-Commerce", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 224-228, September-October 2022.
Journal URL : https://ijsrset.com/IJSRSET229537

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud

Pandiri Manasa[*1], Dr. B. Sasi Kumar[*2]

[*1] M.Tech Student- CSE, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

[*2] Principal & Professor, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

Article Info
Volume 9, Issue 5
Page Number : 229-234

Publication Issue :
September-October-2022

Article History
Accepted : 10 Oct 2022
Published: 30 Oct 2022

ABSTRACT

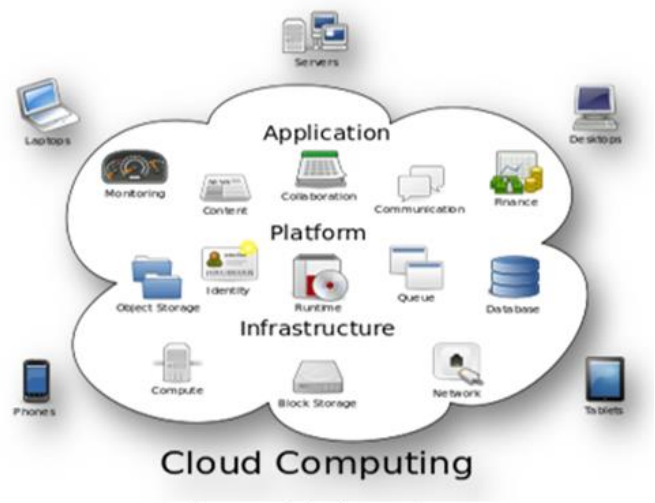
A steadily expanding number of clients should store their data in public cloud servers (PCSs) close to the fast improvement of circulated processing. New security issues ought to be settled to help more clients with taking care of their data straightforwardly cloud. Right when the client is restricted to get to PCS, he will assign its delegate to deal with his data and move them. On the other hand, distant data genuineness checking is moreover a critical security issue without trying to hide conveyed capacity. It makes the clients check whether their reexamined data are kept intact without downloading the whole data. From the security issues, we propose a unique go-between arranged data moving and far away data reliability checking model in character-based public-key cryptography: character-based mediator arranged data moving and far off data uprightness truly investigating straightforwardly cloud (ID-PUIC). We give the legitimate definition, structure model, and security model. Then, a significant ID-PUIC show is arranged using the bilinear pairings. The proposed ID-PUIC show is provably secure considering the hardness of the computational Diffie-Hellman issue. Our ID-PUIC show is in a like manner useful and versatile. Considering the primary client's endorsement, the proposed ID-PUIC show can comprehend private far away data uprightness checking, named far away data trustworthiness checking, and public far off data decency checking.

Keywords : Cloud Computing, Identity-Based Cryptography, Proxy Public Key Cryptography, Remote Data Integrity Checking.

I. INTRODUCTION

Cloud computing (equipment and software) is used and shared remotely over a network in what is known as "the cloud" (usually the Internet). In structure graphs, a cloud-shaped picture is commonly used to represent the complex information it contains, hence the name. Through distributed processing, a client's information, code, and estimation can be shared amongst multiple, geographically dispersed organizations. System hardware and software for appropriate processing are available online from supervised pariah groups.

Modern programming languages and server PC networks are made possible by these establishments.



Structure of cloud computing

Explaining the Workings of Cloud Computing.

Traditional supercomputing, or peak execution handling power, is typically reserved for use by the military and assessment agencies. The purpose of distributed registration is to put this type of processing power to use in client-centric applications, such as financial portfolios, the transmission of updated information, the provision of data limits, and the management of massive, visually impressive PC games. Distributed processing makes use of networks of very large groups of servers, which typically run low-cost client PC development and have some connection to dispersing data-handling tasks. Common IT architectures feature massive aggregations of interconnected systems. Virtualization methods are commonly used to increase the efficiency of distributed computing. Characteristics and Service Types: With the NIST's definitions in mind, here are some of the most remarkable aspects of widely disseminated numbers:

- Self-organization on demand: customer can set their limits for things like server time and association storage as needed, without needing to coordinate with each specialist facility individually.
- Capabilities are accessible over the network and can be used by a variety of client types thanks to standardized frameworks (e.g., cells, PCs, and PDAs).
- Resource pooling: In a multi-tenant model, the provider shares its enlisting resources among its many clients, allocating and reallocating its physical and digital assets to each client by their needs. Since the client generally has no control or data over the specific region of the provided resources at this point, there is a sense of region opportunity and the client may have the option to decide region at a higher level of reflection (e.g., country, state, or server ranch). Resource situations consist of constraints, management, memory, data transmission over networks, and virtual machines.
- Rapid adaptability: Capabilities can be provisioned quickly and skillfully, occasionally normally, to rapidly scale out, and immediately conveyed to rapidly scale in. Often, the client has the impression that they can purchase an unlimited amount of provisioning at any time.
- A metering limit appropriate to the type of business is typically used by cloud architectures to manage and expand resource utilization (e.g., limit, dealing with, information transmission, and dynamic client accounts). Both the user and the resource provider can benefit from due, controlled, and definitive resource use.

Characteristics of cloud computing

II. RELATED WORK

There exist many different security problems in the cloud computing [1], [2]. This paper is based on the research results of proxy cryptography, identity-based public key cryptography and remote data integrity checking in public cloud. In some cases, the cryptographic operation will be delegated to the third party, for example proxy. Thus, we have to use the proxy cryptography. Proxy cryptography is a very important cryptography primitive. In 1996, Mambo et al. proposed the notion of the proxy cryptosystem [3]. When the bilinear pairings are brought into the identity-based cryptography, identity-based cryptography becomes efficient and practical. Since identity based cryptography becomes more efficient because it avoids of the certificate management, more and more experts are apt to study identity-based proxy cryptography. In 2013,Yoon et al. proposed an ID-based proxy signature scheme with message recovery [4]. Chen et al. proposed a proxy signature scheme and a threshold proxy signature scheme from the Weil pairing [5]. By combining the proxy cryptography with encryption technique, some proxy re-encryption schemes are proposed. Liu et al. formalize and construct the attributebased proxy signature [6]. Guo et al. presented a noninteractive CPA(chosen-plaintext attack)-secure proxy reencryption scheme, which is resistant to collusion attacks in forging re-encryption keys [7]. Many other concrete proxy re-encryption schemes and their applications are also proposed [8]–[10]. In public cloud, remote data integrity checking is an important security problem. Since the clients' massive data is outside of their control, the clients' data may be corrupted by the malicious cloud server regardless of intentionally or unintentionally. In order to address the novel security problem, some efficient models are presented. In 2007, Ateniese et al. proposed provable data possession (PDP) paradigm [11].In PDP model, the checker can check the remote data integrity without retrieving or downloading the whole data.PDP is a probabilistic proof of remote data integrity checking by sampling random set of blocks from the public cloud server, which drastically reduces I/O costs. The checker can perform the remote data integrity checking by maintaining small metadata. After that, some dynamic PDP model and protocols are designed [2]–[6]. Following Ateniese et al.'s pioneering work, many remote data integrity checking models and protocols have been proposed [7]–[9]. The end devices may be mobile and limited in computation and storage. Thus, efficient and secure IDPUIC protocol is more suitable for cloud clients equipped with mobile end devices. From the role of the remote data integrity checker, all the remote data integrity checking protocols are classified into two categories: private remote data integrity checking and public remote data integrity checking. In the response checking phase of private remote data integrity checking, some private information is indispensable. On the contrary, private information is not required in the response checking of public remote data integrity checking. Specially, when the private information is delegated to the third party, the third party can also perform the remote data integrity checking. In this case, it is also called delegated checking.

III. SYSTEM ANALYSIS

Existing System Straightforwardly cloud environment, most clients move their data to PCS and truly check out their far-off data's dependability on the Internet. Right when the client is a solitary chairman, a couple of logical issues will happen. Accepting the boss is related to being involved in business coercion, he will be taken out by the police. During the hour of assessment, the boss will be restricted to get to the association to plan for arrangements. In any case, the manager's genuine business will occur during the hour of assessment. When an immense of data is made, who can help him with taking care of this data? In case these data can't be taken care of totally dry on time, the chief will face a lack of monetary interest. To prevent the case from happening, the boss ought to assign a mechanism to deal

with its data, for example, his secretary. However, the head won't believe others can play out the far-away data genuineness checking.

1. Chen et al. proposed a middle-person signature contrive and an edge mediator signature plot from the Weil coordinating.
2. By joining the go-between cryptography with an encryption system, some middle-person re-encryption plans are proposed. Liu et al. formalize and foster the property-based mediator signature.
3. Guo et al. presented a non-natural CPA (picked plaintext attack)- secure delegate re-encryption contrive, which is impenetrable to plot attacks in assembling re-encryption keys.

DISADVANTAGES OF THE EXISTING SYSTEM:

1. Public checking will achieve some gamble of delivering security.
2. Less Efficiency.
3. The security level is low

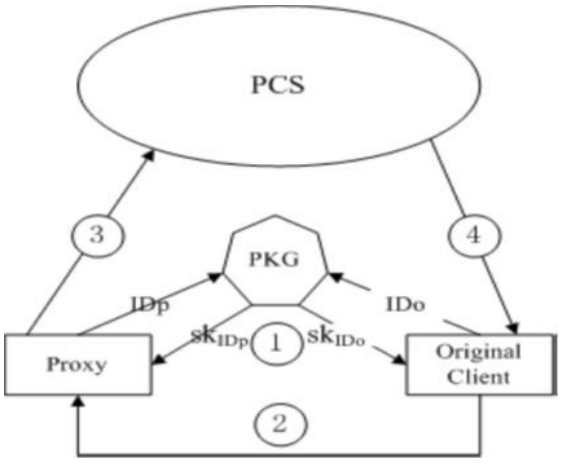
III. PROPOSED SYSTEM

1. This paper relies upon the assessment of eventual outcomes of go-between cryptography, character-based public-key cryptography, and far-off data genuineness investigating transparently cloud.
2. In the public cloud, this paper revolves around character-based delegate arranged data moving and distant data uprightness checking.
3. By using character-based public key cryptology, our proposed ID-PUIC show is successful since the validation the board abstained from. ID-PUIC is a smart go-between arranged data moving and distant data genuineness truly seeing model out in the open cloud. We give the traditional structure model and security model for the ID-PUIC show. Then, considering the bilinear pairings, we arranged the significant ID-PUIC show.
4. In the erratic prophet model, our arranged ID-PUIC show is provably secure. Considering the principal client's endorsement, our show can figure out private checking, relegated checking, and public checking.
5. We propose a successful ID-PUIC show for secure data moving and amassing organization without any attempt at being subtle fogs.
6. Bilinear pairings technique makes character-based cryptography even-minded. Our show depends on the bilinear pairings. We first review the bilinear pairings.

ADVANTAGES OF THE PROPOSED SYSTEM:

1. High Efficiency.
2. Improved Security.
3. The significant ID-PUIC show is provably secure and capable of using legitimate security affirmation and efficiency examination.
4. On the other hand, the proposed ID-PUIC show can in like manner recognize private far-off data decency checking, designated distant data uprightness checking, and public far away data dependability truly investigating perspective on the primary client's endorsement.

IV. SYSTEM DESIGN



MODULES:

1. Original Client
2. Public Cloud Server
3. Proxy
4. KGC

MODULE DESCRIPTIONS:

Stand-out CLIENT:

A surprising Client is an Entity, that will go likely trade an immense information into the public cloud server (PCS) by the doled-out center individual, and the fundamental thing is the validity checking of gigantic information will be through the controller. For the Data moving and Downloading client should follow the going with Process steps:

1. Client can see the cloud chronicles and make the downloading.
2. Client necessities to move the chronicle for specific referred-to credits with the encryption key.
3. Then the client needs to make the mention to the TPA and PROXY to perceive the download endlessly interest for the mystery key which will be given by the TPA.
4. After getting the mystery key client can make the downloading chronicle.
5. Client is an Entity, that will go most likely trade a huge information into the public cloud server (PCS).

PUBLIC CLOUD SERVER: PCS is a part that is remained mindful of by the cloud master affiliation. Laptops are the immense scattered additional room and assessment assets for staying mindful of the client's tremendous information.

Workstations can see the client's all's subtleties and move some records which are valuable for the client and make the cutoff concerning the client moved chronicles.

Go-between: Proxy is a substance, which is upheld to manage the Original Client's information and move them, is picked, and embraced by the Original Client. Precisely when the Proxy fulfills the warrant which is checked and given by the Original Client, it can process and move the essential client's information; if not, it can't do the framework.

Essentially say derives: without the Knowledge of the Proxy's assertion and check and insistence of agent-client can't download the record which is moved by the Client.

V. CONCLUSION

Taking into account the requirements of the applications, this paper suggests the ID-PUIC cloud as the primary form of security. In this paper, we formally present the security model and framework model for ID-PUIC. Next, the bilinear pairings structure is used to arrange the vital ID-PUIC performance. Using the right level of security insistence and proficiency assessment, the essential ID-PUIC demonstration can be demonstrated to be safe and effective. With the help of their essential client, the proposed ID-PUIC display can also detect private distant information validity checking, distributed distant information dependability checking, and public distant information tolerability genuinely researching perspective.

VI. FUTURE WORK

Furthermore, we could attempt to bargain odd circumstances managing associations like glass-breaking parts over high secure cloud framework with the objective that we could deal with the sporadic loss of keys at the information owner's end. This glass-breaking part especially helps in serving the distant clients most genuinely with no assistance breakage regardless of how there is a mix-up occurred at the information proprietor's end because their first-class information related amounted to key difficulty.

VII. REFERENCES

[1]. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, “Achieving efficient cloudsearch services: Multi-keyword ranked search over encrypted cloud datasupporting parallel computing,” IEICE Trans. Commun.,vol.E98-B,no. 1, pp. 190–200, 2015.

[2]. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, “Mutual verifiable provabledata auditing in

public cloud storage," J. Internet Technol., vol. 16, no. 2,pp. 317–323, 2015.

[3]. M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegatingsigning operation," in Proc. CCS, 1996, pp. 48–57.

[4]. E.-J. Yoon, Y. Choi, and C. Kim, "New ID-based proxy signature schemewith message recovery," in Grid and Pervasive Computing (LectureNotes in Computer Science), vol. 7861. Berlin, Germany: Springer-Verlag, 2013, pp. 945– 951.

[5]. B.-C. Chen and H.-T. Yeh, "Secure proxy signature schemes from theweil pairing," J. Supercomput., vol. 65, no. 2, pp. 496–506, 2013.

[6]. X. Liu, J. Ma, J. Xiong, T. Zhang, and Q. Li, "Personal health recordsintegrity verification using attribute based proxy signature in cloudcomputing," in Internet and Distributed Computing Systems (LectureNotes in Computer Science), vol. 8223. Berlin, Germany: Springer-Verlag, 2013, pp. 238–251.

[7]. H. Guo, Z. Zhang, and J. Zhang, "Proxy re-encryption with unforgeablere-encryption keys," in Cryptology and Network Security (Lecture Notesin Computer Science), vol. 8813. Berlin, Germany: Springer-Verlag,2014, pp. 20–33.

[8]. E. Kirshanova, "Proxy re-encryption from lattices," in Public-KeyCryptography (Lecture Notes in Computer Science), vol. 8383. Berlin,Germany: Springer-Verlag, 2014, pp. 77–94.

[9]. P. Xu, H. Chen, D. Zou, and H. Jin, "Fine-grained and heterogeneousproxy re-encryption for secure cloud storage," Chin. Sci. Bull., vol. 59,no. 32, pp. 4201–4209, 2014.

[10]. S. Ohata, Y. Kawai, T. Matsuda, G. Hanaoka, and K. Matsuura,"Re-encryption verifiability: How to detect malicious activities of aproxy in proxy re-encryption," in Proc. CT-RSA Conf., vol. 9048. 2015,pp. 410–428.

Cite this article as :

Pandiri Manasa, Dr. B. Sasi Kumar, "Identity-Based Proxy-Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 229-234, September-October 2022.

Journal URL : https://ijsrset.com/IJSRSET229538

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Providing Cloud Storage Auditing Through Verifiable Key Update Outsourcing

P Sanjana[*1], Dr. B. Sasi Kumar[*2]

[*1] M.Tech Student- CSE, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

[*2] Principal & Professor, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

Article Info
Volume 9, Issue 5
Page Number : 235-239

Publication Issue :
September-October-2022

Article History
Accepted : 10 Oct 2022
Published: 30 Oct 2022

ABSTRACT

In many security applications, key-exposure resistance has long been a pressing concern for a comprehensive cyber defence strategy. How to address this critical exposure issue in the context of cloud storage auditing has been proposed and investigated as of late. Existing solutions to the problem necessitate that the client updates his secret keys at regular intervals, which can be a significant burden for clients with limited computational resources, like mobile phones. To provide maximum client transparency during key updates, we propose a novel paradigm in this paper: cloud storage auditing combined with the verifiable outsourcing of key updates. In this model, the client doesn't have to worry about keeping track of key updates because they can be safely delegated to a trusted third party. In particular, we adapt the role of the third-party auditor (TPA) from numerous existing public auditing designs, giving it responsibility for both the auditing of the storage and the security updates of keys in order to prevent key exposure. Our scheme requires TPA to keep only an encrypted copy of the client's secret key while performing these otherwise onerous tasks on the client's behalf. When transferring data to the cloud, the client only needs to get the encrypted secret key from the TPA. Further, our architecture provides the client with the means to confirm the authenticity of the TPA's supplied encrypted secret keys. The whole auditing process with key exposure resistance is made as clear to the client as possible by the inclusion of these prominent features. The definition and underlying security model of this paradigm are formally outlined. Our rigorously tested and simulated implementations of the detailed designs have proven to be safe and effective in practice.

Keywords : Cloud Storage, Outsourcing Computing, Cloud Storage Auditing, Key Update, Verifiability.

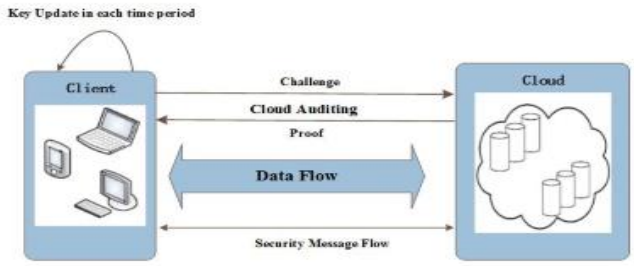
I. INTRODUCTION

One of the most crucial safety measures in cloud storage is auditing, which is implemented to ensure the authenticity of information kept in the cloud. Recent years have seen extensive studies into the topic of auditing protocols for cloud storage. One of the primary concerns of these protocols is how to achieve high bandwidth and computation efficiency, which is relevant to the auditing process as a whole. Therefore, the Homomorphism Linear Authenticator (HLA) technique is investigated, as it allows the auditor to verify the integrity of the data in the cloud without retrieving the whole data, thus reducing the computational and communication overheads of auditing protocols.

Many auditing protocols for cloud storage like have been proposed using this method. Auditing of cloud storage services should also take privacy measures seriously. A third-party auditor (TPA) is introduced to assist the client in performing periodic checks of the cloud's data integrity, thereby reducing the client's computational burden. After the TPA has executed the auditing protocol multiple times, it may be able to obtain the client's data. Client data in the cloud is kept private using auditing protocols. What's more, the auditing of cloud storage has addressed the question of how to facilitate data-dynamic operations.

In this project, we introduce the concept of an auditing protocol with key-exposure resilience and conduct the first research into its implementation for a storage auditing system. In such a protocol, even if the cloud acquires the client's current secret key for cloud storage auditing, any dishonest behavior, such as deleting or modifying some clients' data stored in the cloud in previous periods, can be detected. Existing designs for auditing protocols do not account for this crucial shortcoming. For safe cloud-based data storage, we formalize the definition and security model of auditing protocols with key-exposure resilience.

For the first time, we create a practical auditing protocol for cloud storage that includes built-in resistance to key exposure. The binary tree structure, used in a variety of earlier works on various cryptographic designs, is put to use here to accomplish our goal of keeping the client's secret keys secure and up to date. One could think of this binary tree structure as a subset of the tree structure employed by the HIBE scheme. Additionally, a binary tree's nodes are linked to their respective periods using the preorder traversal method. To implement the binary tree preorder traversal in our detailed protocol, we make use of the stack data structure.



1. System model of our cloud storage auditing

Using the system described below, we investigate the possibility of outsourcing numerical and logical computations. If a customer needs calculations performed but their internal resources (computer power, appropriate software, or programming skills) are insufficient, they may turn to an external operator for help. These days, we see this in a wide variety of everyday contexts, from fiscal to oil administrations. If the outsourcing is handled so that neither the original data nor the final calculation results are revealed to the third party, then it is considered a safe practice. The basic idea is that the client should perform some carefully planned local preprocessing (masking) of the problem or potentially information before sending it to the operator and that the client should also perform some carefully planned local postprocessing of the appropriate response come back to extract the true reply. As little effort as possible should be put into the camouflage process regarding the size of the information and the response. Numerical

computational performance may be altered by the camouflage preprocessing that the client performs locally to "conceal" the real calculation. Here, we present a structure for hiding logical computations and discuss their prices, numerical properties, and degrees of security. These covert operations can be set up in a normal state, a user-friendly framework (critical thinking condition), which conceals their complexity. We provide protocols for the secure and private outsourcing of direct polynomial math computations, allowing a client to safely outsource expensive logarithmic computations (such as the expansion of large-scale systems) to two remote servers while ensuring that neither server can learn anything about the client's private information or the result of the computation. The customer's local computations are efficient in the scope of their information and don't necessitate any time-consuming or money-sucking encryptions of the customer's input. The computational burden on the servers is proportional to the time unpredictability of the currently practically used calculations for addressing the arithmetic problem (e.g., relative to n3 for increasing two n x n networks). Even if the servers were to collude against the client, they could only learn where the client gets their information, but they couldn't change the correct response without the client knowing.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

One of the most valued aspects of cloud computing is cloud storage. However, while cloud storage solves many problems for its users, it also introduces new security issues. How to efficiently verify the authenticity of cloud-based data is a pressing issue in information security. Many auditing protocols for cloud storage have been proposed to address this issue in recent years. Another critical issue with auditing cloud storage is the 'key exposure problem.'

Problems with the Current System:

1. Ineffectiveness of data integrity checks
2. If the cloud gains access to the client's secret key for storage auditing, it can easily cover up any data loss incidents, protect its reputation, and get rid of the client's infrequently used data to free up space.

PROPOSED SYSTEM

A new paradigm is proposed, one that combines the auditing of cloud storage with the verifiable outsourcing of key updates. In the new model, the client no longer performs key-update operations but rather is an authorized third party. An authorized third party keeps the client's encrypted secret key and updates it each period for use in auditing cloud storage. If and when the client needs to upload new files to the cloud, he will need to download the encrypted secret key from the authorized party and decrypt it. The client also can validate the authenticity of the encrypted secret key. In this work, we develop the first auditing protocol for cloud storage that allows for the dependable delegation of key updates. Our architecture positions the TPA as the official custodian of all necessary revisions. Another crucial duty of the TPA is to verify the authenticity of the client's cloud-based data, much like the traditional public auditing protocols. Since the TPA only has an encrypted copy of the client's secret key, it cannot perform an audit of the client's cloud storage without access to the client's private key. To protect the TPA's private keys, we employ an encryption algorithm based on the blinding technique, which uses the homomorphic property. It improves the safety of our protocol and the speed of the decryption procedure. The TPA, meanwhile, can finish up any necessary key updates while in an encrypted state. After receiving the encrypted secret key from the TPA, the client can check its authenticity.

The Benefits of the Suggested Method:

1. The client is not aware of the TPA's handling of key updates in this protocol.
2. The TPA is only privy to the encrypted client secret key, and the client can double-check the TPA's encryption after it has downloaded the keys.

III. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE:

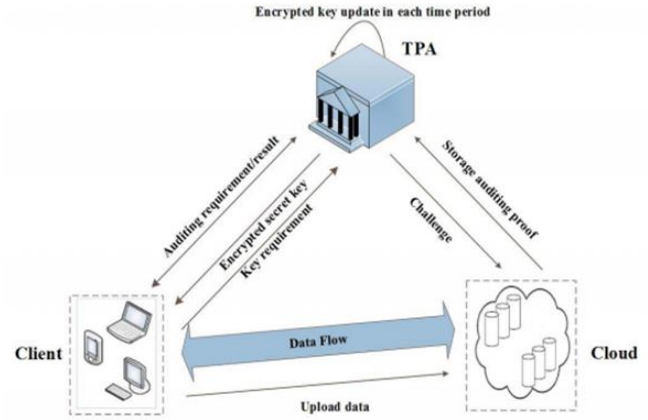


Fig. 1. System model of our cloud storage auditing.

MODULES

We have 3 main modules in this project;

1. Client Module
2. Cloud Module
3. Third Party Auditor (TPA)

Client:

The client retains all legal rights to any data stored in the cloud. Rather than having a set total size, the client can upload the expanding files to the cloud at any time.

Cloud:

The cloud serves as a repository for the client's data and a download hub.

TPA:

The TPA's primary function is to conduct an audit of the client's cloud-based data files, and its secondary function is to periodically update the client's encrypted secret keys.

IV. CONCLUSION

To better protect our clients, we investigate the most vulnerable areas of their cloud storage accounts. An auditing protocol with key-exposure resilience is the new paradigm we propose. In such a protocol, even if the client's current secret key for cloud storage auditing is compromised, the data's integrity can still be verified for data that was previously stored in the cloud.We propose the first operational solution after formally defining and modelling the security of an auditing protocol that is resistant to key exposure. The proposed protocol is demonstrated to be safe and effective through proof of security and an analysis of its asymptotic performance.

V. FUTURE WORK

The generation of the time period key is not something we suggest should be based on operations but on logging instead. It's inefficient to generate new keys all the time, so long periods of time between them are recommended instead. Automatically, based on a predetermined time period, a new key should be generated.

VI. REFERENCES

[1]. M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," Adv. Comput., vol. 54, pp. 215–272, 2002.

[2]. D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. 6th Annu. Conf. Privacy, Secur. Trust, 2008, pp. 240–245.

[3]. C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in

cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.

[4]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Secur., 2012, pp. 541–556.

[5]. G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.

[6]. A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

[7]. H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.

[8]. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.

[9]. F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2008.

[10]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiplereplica provable data possession," in Proc. 28th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.

Cite this article as :

P Sanjana, Dr. B. Sasi Kumar, "Providing Cloud Storage Auditing Through Verifiable Key Update Outsourcing", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 235-239, September-October 2022.

Journal URL : https://ijsrset.com/IJSRSET229539

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Wireless Sensor Networks with Efficient Clone Detection in Terms of Energy and Memory

Sana Afia[*1], Dr. B. Sasi Kumar[*2]

[*1] M.Tech Student- CSE, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

[*2] Principal & Professor, Department of Computer Science Engineering, Dr. V. R. K. Women's College of Engineering & Technology, Hyderabad, Telangana, India

Article Info
Volume 9, Issue 5
Page Number : 240-247

Publication Issue :
September-October-2022

Article History
Accepted : 10 Oct 2022
Published: 30 Oct 2022

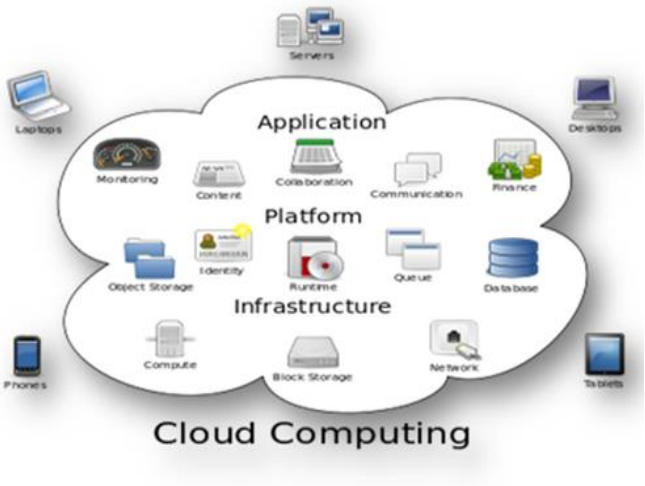
ABSTRACT

We propose an energy-efficient location-aware clone detection protocol for densely deployed WSNs to ensure successful clone attack detection and satisfactory network lifetime. Using the sensors' geolocation data, we randomly select witnesses within a ring area to attest to the sensors' legitimacy and report any clone attacks they may have uncovered. The witnesses and the sink along the path can receive data with minimal power consumption thanks to the ring topology. For the first time, we theoretically show that the proposed protocol can achieve a clone detection probability of one hundred percent with trustworthy witnesses. In this expanded work, we examine clone detection performance with untrustful witnesses and find that, even with 10% of witnesses being compromised, the clone detection probability is still very close to 99%. The proposed protocol also requires buffer storage of sensors that depends not on the number of sensors, n, but on the network's radius, h, i.e. Oh, whereas the required buffer storage of sensors is typically dependent on the node density in existing clone detection protocols with random witness selection scheme. Extensive simulations show that our proposed protocol can ensure a long network lifetime by evenly distributing the traffic load across the network.

Keywords : Wireless Sensor Networks, Clone Detection Protocol, Energy Efficiency, And Network Lifetime

I. INTRODUCTION

Cloud computing (equipment and software) is used and shared remotely over a network in what is known as "the cloud" (usually the Internet). In structure graphs, a cloud-shaped picture is commonly used to represent the complex information it contains, hence the name. Through distributed processing, a client's information, code, and estimation can be shared amongst multiple, geographically dispersed organizations. System hardware and software for appropriate processing are available online from supervised pariah groups. Modern programming languages and server PC networks are made possible by these establishments.



Structure of cloud computing

Explaining the Workings of Cloud Computing

Traditional supercomputing, or peak execution handling power, is typically reserved for use by the military and assessment agencies. The purpose of distributed registration is to put this type of processing power to use in client-centric applications, such as financial portfolios, the transmission of updated information, the provision of data limits, and the management of massive, visually impressive PC games. Distributed processing makes use of networks of very large groups of servers, which typically run low-cost client PC development and have some connection to dispersing data-handling tasks. Common IT architectures feature massive aggregations of interconnected systems. Virtualization methods are commonly used to increase the efficiency of distributed computing. Characteristics and Service Types: With the NIST's definitions in mind, here are some of the most remarkable aspects of widely disseminated numbers:

- Self-organization on demand: customer can set their limits for things like server time and association storage as needed, without needing to coordinate with each specialist facility individually.
- Capabilities are accessible over the network and can be used by a variety of client types thanks to standardized frameworks (e.g., cells, PCs, and PDAs).
- Resource pooling: In a multi-tenant model, the provider shares its enlisting resources among its many clients, allocating and reallocating its physical and digital assets to each client by their needs. Since the client generally has no control or data over the specific region of the provided resources at this point, there is a sense of region opportunity and the client may have the option to decide region at a higher level of reflection (e.g., country, state, or server ranch). Resource situations consist of constraints, management, memory, data transmission over networks, and virtual machines.
- Rapid adaptability: Capabilities can be provisioned quickly and skillfully, occasionally normally, to rapidly scale out, and immediately conveyed to rapidly scale in. Often, the client has the impression that they can purchase an unlimited amount of provisioning at any time.
- A metering limit appropriate to the type of business is typically used by cloud architectures to manage and expand resource utilization (e.g., limit, dealing with, information transmission, and dynamic client accounts). Both the user and the resource provider can benefit from due, controlled, and definitive resource use.

Characteristics of cloud computing

II. RELATED WORK

2.1 Protocol for detecting clones in wireless sensor networks that uses minimal power (ERCD)

Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen are the authors here.

As their capabilities continue to improve, wireless sensor networks (WSNs) are finding use in a growing number of fields, from the study of dangerous environments to the delivery of medical care remotely. However, due to hardware and cost limitations, sensors are vulnerable to clone attacks, which presents significant obstacles to developing and deploying an energy-efficient WSN. In this paper, we propose a location-aware clone detection protocol that can reliably identify clone attacks while minimizing their impact on the longevity of the network. To confirm sensor privacy and identify clone attacks, we utilize sensor location data and randomly select witness nodes in a ring area. Traffic load is spread out across the network, increasing network lifetime, and the ring structure allows for energy-efficient data forwarding along the path to the witnesses and the sink. Analyses and simulations show that the proposed protocol can nearly achieve a perfect clone detection probability with reliable witnesses. We further extend the work by investigating the performance of clone detection with untrustworthy witnesses, and we find that even when 10% of witnesses are compromised, the clone detection probability is still close to 98%. Moreover, in comparison to the current method, our proposed protocol can greatly increase the network's lifetime.

2. Sustainability, dependability, and safety in the next generation of M2M communications are the focus of Section 2.2 GRS.

R. Lu, X. Li, X. Liang, X. Shen, and X. Lin are the authors.

Communication between machines is characterized by a large number of autonomous machines exchanging data and reaching collective conclusions without the involvement of a human hand. M2M communications have become a game-changer for many real-time monitoring applications like remote e-healthcare, smart homes, environmental monitoring, and industrial automation because of their potential to support a large number of ubiquitous characteristics and achieve better cost efficiency. Nonetheless, the success of M2M communications depends on overcoming the current obstacles of green energy consumption, unreliable connections, and insecure data (GRS). No serious adoption of M2M communications as a promising communication paradigm can occur without GRS guarantees. This article's goal is to promote an energy-efficient, reliable, and secure M2M communications environment by examining the emerging field from the perspective of potential GRS issues. To be more precise, we first formally define GRS requirements by incorporating three domains into the M2M communications architecture: the M2M domain, the network domain, and the application domain. We then investigate activity scheduling, redundancy utilization, and cooperative security mechanisms as several GRS enabling techniques. These methods show potential for speeding up the creation and rollout of M2M communications software.

3 A review of wireless sensor networks

W. Su, Y. Sankarasubramaniam, E. Cayirci, and I. F. Akyildiz are the authors.

Applications such as remote environmental monitoring and target tracking are crucial uses for a wireless sensor network (WSN). This has been made possible by the development in recent years of increasingly affordable miniaturized and computationally capable sensors. These sensors can form a network by talking to one another through their built-in wireless interfaces. Environment, application design goals, cost, hardware, and system constraints are just some of the factors that must be taken into account when planning a WSN's architecture.

We divide the issues into three groups:

(1) The core infrastructure and OS,

(2) The communication protocol stack, and

(3) The network infrastructure and its deployment

And maintenance. We summarise the most significant progress made in these three areas and describe forthcoming difficulties.

4. Cost-function-based energy-aware routing algorithms for wireless sensor networks: design principles and enhancements

PUBLISHER(S): A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen

To increase the network's efficiency with energy and to lengthen its lifespan, cost-function-based problem's complexity means that the current approaches all have their drawbacks. This paper examines the fundamentals, design principles, and evaluation techniques of cost-function-based routing algorithms. This paper proposes two cost-based routing algorithms that are also energy-aware: the Exponential and Sine Cost Function based Route (CFR) and the Double Cost Function based Route (DCFR). ESCFR's cost function can translate incremental shifts in nodal remaining energy to sizable shifts in overall function value. DCFR's cost function considers both the total energy used and the amount of energy left in each node, leading to a more efficient and equitable distribution of power. Analysis of the effectiveness of the cost function architecture is performed. Extensive simulations show the proposed algorithms outperform their rivals by a wide margin.

5 Using dispersed random paths for secure data collection in wireless sensor networks

T. Shu, M. Krunz, and S. Liu are the authors.

Key attacks in wireless sensor networks include compromised nodes and denial of service (WSNs). In this paper, we explore data delivery mechanisms that have a good chance of avoiding the black holes created by these attacks.

As a result of their deterministic nature, multipath routing approaches are susceptible to such attacks. Therefore, all data transmitted over these routes are open to attack once the adversary obtains the routing algorithm and can compute the same routes as the source. In this paper, we create a system to generate multipath routes at random. When implemented, our plans call for different packet "shares" to take different paths at different times. Therefore, the adversary cannot determine the paths taken by each packet even if the routing algorithm is compromised. The routes generated are not only completely random but also highly dispersed and energy efficient, making them more than capable of avoiding black holes. We perform an analytical study on the safety and efficiency of the proposed schemes. In addition, we formulate an optimization problem to reduce overall power usage while maintaining specified levels of safety. In-depth simulations are run to ensure the accuracy of our mechanisms.

III. SYSTEM ANALYSIS

3.1 Existing System

A group of nodes (witnesses) is typically chosen to attest to the network's nodes' authenticity in order to facilitate efficient clone detection. During the witness selection phase, the source node's identity and location are revealed to the witnesses. If a network node fails a certification check, the witnesses will report an attack. For clone detection to be successful, two criteria should be met in the selection and verification of witnesses:

1) It's necessary to choose witnesses at random;

2) At least one of the witnesses can receive the verification message(s) for detecting clones.

3) Threatening the efficient operation of WSNs are issues such as the uneven energy consumption of protocols like Randomized Efficient and Distributed (RED) and Line-Select Multicast (LSM), and the possibility of network partition brought on by dead sensors. Threatening the efficient operation of WSNs are issues such as the uneven energy consumption of protocols like Randomized Efficient and Distributed (RED) and Line-Select Multicast (LSM), and the

possibility of network partition brought on by dead sensors.

3.2 THE FLAWS IN THE CURRENT SYSTEM:

- Existing infrastructure does not guarantee that at least one witness can verify sensor node identities in the event of a clone attack; our goal, therefore, is to make it hard for malicious users to eavesdrop on the communication between the current source node and its witnesses.
- These requirements are critical but challenging to meet in clone detection protocol design, as they do not guarantee a high clone detection probability (the likelihood that clone attacks will be detected).
- When designing clone detection protocols for sensor networks, it is important to consider the energy and memory efficiency of sensors as well as to establish criteria that will lead to high performance in terms of clone detection probability.
- When a sensor's battery life starts to get low, it's important to make sure that sensors across the network are using their power efficiently and cooperatively.

3.3 PROPOSED SYSTEM

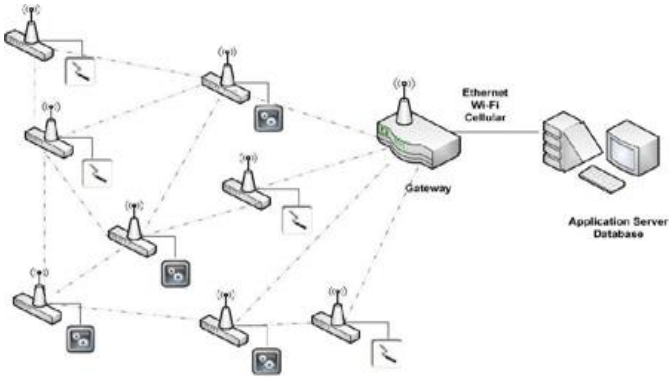
- For WSNs, we consider energy efficiency and memory needs alongside the clone detection probability as we design a distributed clone detection protocol with a random witness selection scheme.
- Our protocol can be used in networks with many nodes, such as multi-hop WSNs, and in which sensor nodes may be compromised or cloned by attackers.
- To further our analytic model, we evaluate the data buffer needs of the ERCD protocol and supplement our theoretical analysis with experimental results. The Powerful Method for Identifying Clone Rings.
- We find that the ERCD protocol can balance the energy consumption of sensors in different locations by spreading the witnesses across WSNs, with the exception of the non-witness rings, i.e. the adjacent rings around the sink, which should not have witnesses.
- Then, we use the energy budget to find the sweet spot for the number of rings that don't count as witnesses.
- Finally, we demonstrate the scalability of our proposed protocol by demonstrating that the required buffer size depends only on the size of the ring, an expression we derive using the ERCD protocol.

3.4 BENEFITS OF THE INTENDED SYSTEM:

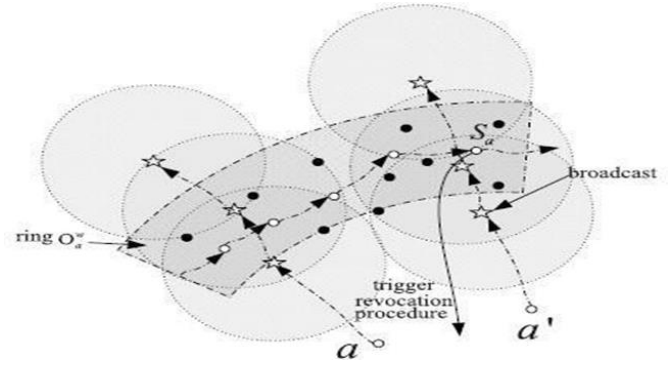
- The efficiency of the ERCD protocol is evaluated by examining its ability to detect clones, energy consumption, network lifetime, and buffer capacity.
- Our proposed ERCD protocol outperforms state-of-the-art solutions in terms of clone detection probability and network lifetime while keeping data throughput under control, as shown by extensive simulation results. This study demonstrates that even with unreliable witnesses, the probability of detecting a clone can approach 100%.
- The ERCD protocol reduces traffic of witness selection and legitimacy verification for sensors close to the sink, which helps to even out the energy consumption of data collection.

IV. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE



BLOCK DIAGRAM



MODULES

• Module for System Construction

• Protocol for Early Reproductive and Child Determination

• Clone Detection Likelihood

• Concerns about longevity and energy use in networks Module for Building Systems

• To test and implement our proposed system, we create the "System Construction Module" in the first phase of development. We take into account a network environment with a single base station (BS) and a huge number of wireless sensor nodes.

• The sink node acts as the coordinator's starting point. The network area is virtually divided into contiguous rings based on the location of the BS, with the width of each ring equal to the range of transmission of sensor nodes. The network is a densely deployed WSN in the sense that there are sensor nodes in each of the rings adjacent to each node, and ii) there are sufficient sensor nodes in each ring to build a routing path along the ring.

• The network model can be easily extended to accommodate scenarios with more than one BS, each of which would communicate with its corresponding sensor nodes using orthogonal frequency-division multiple-access (OFDMA). Each sensor needs to be able to collect data and identify duplicates. Every time a sensor completes a data cycle, it sends its findings to the "sink node" via a series of intermediate nodes.

• To allow any node to be chosen as a witness, the buffer space must be large enough to store the secret data of all source nodes. As new data arrives at the sensor node, the oldest data will be discarded until space is available in the buffer.

The ERCD Protocol

• In this section, we present our ERCD protocol, a distributed clone detection method that requires few buffers and has a low impact on the lifetime of the network.

• There are two phases to the ERCD protocol: choosing witnesses and checking their credentials. Each source node uses a random mapping function to choose its witnesses at random during the witness selection process. During legitimacy verification, the source node sends out a verification request to its witnesses that includes the source node's sensitive data. Once witnesses have received the verification messages, they will forward them to the witness header for legitimacy verification. The witness header is the node responsible for determining whether or not the source node is legitimate by comparing the collected messages from all witnesses. The witness header will notify the sink of a clone attack and initiate a revocation process if the received messages do not match the existing record or have expired.

Clone Detection Probability

• In this lesson, we'll look at how to design a distributed clone detection protocol with random witness selection by balancing the likelihood of finding a clone, the expected lifespan of the network, and the capacity

of any data buffers. At first, only a handful of nodes are taken over by bad actors. Using the clone detection protocol, we seek to maximize the clone detection probability or the likelihood that a cloned node will be discovered; simultaneously, sufficient energy and buffer storage capacity for data collection and operating the clone detection protocol should be guaranteed, which means that the network lifetime, or the time from when the network is first activated until the first outage occurs, should not be irrationally short.

• The clone detection probability in a randomly selected set of witnesses for a distributed clone detection protocol is dependent on the likelihood that those witnesses will actually receive the verification message from the source node. Therefore, ERCD's clone detection probability protocol refers to the likelihood that the verification message will be delivered successfully from the source node to its witnesses.

• In order to ensure the safety of the network, the ERCD protocol broadcasts the verification message whenever it is in close proximity to the witness ring.

Power Use and Longevity of a Network

• Since wireless sensor nodes in WSNs are typically powered by batteries, it is crucial to assess the energy requirements of sensor nodes and guarantee that normal network operations will not be disrupted in the event of a node failure. For the purpose of measuring the efficacy of the ERCD protocol, we define the network lifetime as the time span between the first moment of network operation and the occurrence of any node outage.

• With reception accounting for such a small share of overall power usage, we focus solely on transmission power consumption. Due to the ring-based nature of the generation of witness sets in our ERCD protocol, sensor nodes within the same ring perform similar functions. The analysis is simplified by assuming that all sensor nodes within the same ring experience the same volume of traffic.

• Our work here is generic in that it can be applied to a wide range of energy models, and this is one of its main selling points. Nodes in rings with indices less than or equal to k are considered to be inside the ring, while nodes in rings with indices greater than or equal to k are considered to be outside the ring. In order to calculate energy consumption and network lifetime, we first examine the traffic load of each sensor node. Using the ERCD protocol, the typical data collection, witness selection, and authenticity verification tasks are distributed evenly across all sensor nodes.

IV. CONCLUSION

In this paper, we propose a distributed, low-energy protocol for detecting clones by randomly selecting witnesses. We have proposed the ERCD protocol, which involves the steps of selecting witnesses and verifying their credibility. Since each sensor node's witnesses are dispersed in a ring structure, detecting a clone attack is straightforward via verification message, as shown by our theoretical analysis and simulation results. In addition, with a sufficient amount of data buffer, our protocol can extend the life of the network and reduce the total amount of energy used. This is because we make use of the location data to disperse the traffic load across WSNs, relieving the burden on the sensor nodes near the sink node's energy consumption and memory storage while simultaneously increasing the network's lifespan. As we move forward, we plan to take into account a wide range of mobility trends across numerous network configurations.

V. FUTURE WORK

In the future, we will take into account varied mobility patterns across a range of network conditions in our upcoming work. The ability to encrypt packets as they are being transferred to the destination can also be

added, enhancing security and reducing the risk of internal attacks brought on by network sensor nodes.

VI. REFERENCES

[1]. Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in wasns," in Proc. IEEE INFOCOM, Turin, IT, Apr. 14- 19 2015, pp. 2436–2444.

[2]. R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," IEEE Communications Magazine, vol. 49, no. 4, pp. 28–35, Apr. 2013.

[3]. Christo Ananth, A.NasrinBanu, M.Manju, S.Nilofer, S.Mageshwari, A.PeratchiSelvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2012,pp:16-19

[4]. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," Computer Networks, vol. 56, no. 7, pp. 1951–1967, May. 2011.

[5]. T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sen-sor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6]. Uma Vasala and Dr. G. R. Sakthidharan," Effective Key Management In Dynamic Wireless Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.4, no.7, pp. 308- 312, 2017.

[7]. K.MANIMALA and .RANJITH," Mobile Transmission Using Rigorous Data for Wireless Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 436- 446, 2014.

[8]. P. G. V. SURESH KUMAR1 , SEELAM SOWJANYA," Developing An Enterprise Environment by Using Wireless Sensor Network System Architecture"..”International Journal of Computer Engineering in Research Trends., vol.2, no.10, pp. 902- 908, 2015.

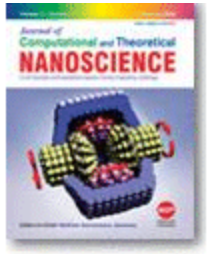
[9]. JALAGAM NAGAMANI, K.SUMALATHA," EAACK: Secure IDS for Wireless Sensor Networks"..”International Journal of Computer Engineering in Research Trends., vol.1, no.6, pp. 461- 469, 2014.

[10]. G V N LAKSHMI PRIYANKA, TELUGU KAVITHA, B SWATHI and P.SUMAN PRAKASH," Significance of DSSD towards Cut Detection in Wireless Sensor Network"..”International Journal of Computer Engineering in Research Trends., vol.2, no.1, pp. 8-12, 2015.

Cite this article as :

Sana Afia, Dr. B. Sasi Kumar, "Wireless Sensor Networks with Efficient Clone Detection in Terms of Energy and Memory", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 240-247, September-October 2022.

Journal URL : https://ijsrset.com/IJSRSET229540



Restrictive Ambiguity and Add-On Architecture Prototype for Privacy Preservation in Cloud Auditing

Authors: Mohammed, Akheel [1] ; Vasumathi, D [2] ;
Source: Journal of Computational and Theoretical Nanoscience, Volume 15, Number 8, August 2018, pp. 2565-2571(7)
Publisher: American Scientific Publishers
DOI: https://doi.org/10.1166/jctn.2018.7499

This paper encompasses an architecture that allows processing of larger voluminous data and restricting the confidential data from being revealed to unreliable sources. The system is a modular and enables segmentation into components of varying importance, depending on the credibility of information. Clouds architecture following this set up will have an internet connected add-on segments of spaces for individual users. This segmentation will limit the option of public auditors to access certain data which belongs to user carefully categorized by themselves into protected segments. Resource allocation and retrieval of user data from Cloud Service provider (CSP) will also be efficient. From the obtained result, it is evident that communication overhead will be reduced as resource allocation will be having less latency in a modular architecture. Secondly, a data owner will be having the rights in selecting and providing the content for auditing to the Public Auditing tool. This enhances the security implementation of a modular architecture. Restrictive ambiguity is to ensure that the