CLOUD COMPUTING SECURITY CHALLENGES, THREATS AND VULNERABILITIES

[1]PITTALA RAJKUMAR, [2]Dr. S. THAIYALNAYAKI, [3]CHINAGOUNI PAVAN KUMAR REDDY, [4]SADENENI HARSHITH, [5]KAMBAGONI SANDEEP KUMAR

[1,3,4,5]STUDENT, [2]ASSOCIATE PROFFESSOR
BHARATH INSTITUTE OF HIGHER EDUCATION AND RESEARCH

Abstract- **Today data sharing and maintaining its security is major challenge. User in the data sharing system upload their file with the encryption using private key. This property is especially important to any large-scale data sharing system, as any user leak the key information then it will become difficult for the data owner to maintain security of the information. In this paper provide a concrete and efficient instantiation of scheme, prove its security and provide an implementation to show its practicality. There are lots of challenges for data owner to share their data on servers or cloud. There are different solutions to solve these problems. These techniques are very much critical to handle key shared by the data owner. This paper will introduce the trusted authority to authenticate user those who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system. Trusted authority send file to CSP module to store on cloud. The resulting key sets are shown to have a number of desirable properties that ensure the confidentiality of communication sessions against collusion attacks by another network node.**

CHAPTER I
INTRODUCTION

In computer technological know-how, cloud computing describes a rising computer carrier, just like how an energy deliver is became off. That's simply the way it's far. We don't should fear about in which the energy comes from, how it's made or transported. Each month they pay what they eat. The concept behind cloud computing is similar: the user can sincerely use garage, computing energy, or a custom-built development environment without worrying about how they work internally. Cloud computing is essentially internet computing. The cloud is a metaphor for the Internet primarily based on how the Internet is defined in computer community diagrams; which means that that abstraction that hides the complicated infrastructure of the Internet. It is a technique of computing wherein relevant resources are furnished "as a carrier", allowing users to access technological services from the Internet ("inside the cloud") without information or manage over the technologies underlying those servers. Cloud computing may be found out in each huge cloud systems and massive facts systems, implying increasing problems in objective get right of entry to to statistics. This results in insufficient nice of acquired content. The effect of cloud computing on cloud computing and large information systems can fluctuate. However, a common thing that may be highlighted is the quandary in the particular distribution of content material, a problem to be solved by means of growing metrics that attempt to improve accuracy. A cloud network consists of a manage plane and a statistics aircraft. For example, on the information stage, cloud computing lets in computing offerings to reside at the threshold of a network rather than on servers in a information center. Compared to cloud computing, cloud computing emphasizes proximity to quit users and consumer objectives, dense geographic distribution and neighborhood aid sharing, latency reduction and traffic financial savings to improve excellent of carrier (QoS) and analytical facet/analytical drift, which bring about better. Consequences person usage and redundancy in case of failure, in addition to the capability to use AAL in scenarios.

OBJECTIVE

The important reason of the machine is to provide a concrete and effective implementation environment, to show its protection, and to ensure that it demonstrates its concreteness. The foremost purpose of this system is that the relied-on authority uses the SHA set of rules to generate the important thing and this key could be shared with the consumer in addition to the proprietor. The credit authorities module receives the encrypted document using the AES set of rules from the records owner and calculates the fee of the deduction the use of the MD-V algorithm.

CHAPTER II
LITERATURE REVIEW

2.1 Efficient and Verifiable Outsourcing scheme of Sequence Comparisons

With the fast improvement of cloud computing, techniques of accurately freeing prohibitively high-priced computing are spreading attention in the medical network. In the great computing paradigm, clients with constrained assets can increase heavy computing obligations to a cloud server and revel in unlimited computing assets on a pay-as-you-go basis. One of the most vital functions of outsourced accounting is the ability to confirm results.

2.2 Secure outsourcing of the following preparations

One of the primary capabilities of statistics outsourcing is the capability to validate. However, there are very few relaxed mechanisms for selling serial comparison clients to check whether the servers are following the suitable protocol or not. In this

newsletter, we can clear up this problem with the aid of integrating the deformable scheme technique with homomorphic encryption. Compared to present schemes, our proposed solution allows clients to efficiently stumble on server corruption.

2.3 Comparison of secured and closed sequences

The amount of communication finished by means of our protocol is proportional to the time complexity of the exceptional-regarded set of rules for performing the series comparison. The hassle of determining the similarity of two sequences arises in lots of applications, specially in bioinformatics. In those application regions, one of the concepts of series similarity is widely used to edit the distance: it is the collection of insertions, deletions and substitutions at the bottom fee required to convert one string into every other.

2.4 A new modular algorithm for secure outsourcing exposure

The exponentiation of the modular operation is taken into consideration to be the most valuable in cryptographic protocols primarily based on the discrete logarithm. In this paper, we endorse a brand new relaxed distribution set of rules for the modular exponent of a prime number in a model with a unmarried malicious code. Compared with the cutting-edge algorithm, the proposed set of rules is superior in each performance and verifiability. We consequently use this algorithm as a recurring for Cramer-Shop encryption and Schnarr signatures to provide safety from outside sources. In addition, we advocate the first relaxed and efficient set of rules for simultaneous modular exponents.

CHAPTER III
EXISTING SYSTEM

Big issues in the bodily and existence sciences are being addressed with the aid of Internet computing technologies, inclusive of Performance computing, which permit the sharing of computing strength, bandwidth, garage, and facts. A susceptible computing machine as soon as related to such a community is now not confined via its slow velocity, small nearby reminiscence and constrained bandwidth: it is able to use the abundance of these assets available some other place inside the network. An impediment to using "computing outsourcing" is that the records in question is frequently sensitive, as important to countrywide safety, or is proprietary and consists of exchange secrets and techniques, or need to be saved personal by way of criminal necessities, inclusive of HIPAA, Gramm. -Leach-Bliley, or comparable laws. This development stocks the incentive of computing systems with privateness, that is, without far off agents whose computing energy is used, neither their own statistics nor the consequences of calculations on the statistics.

DISADVANTAGES OF THE EXISTING SYSTEM

- Secure outsourcing for a common set of contribution obligations
- The threat of leakage is indicated through the statistics

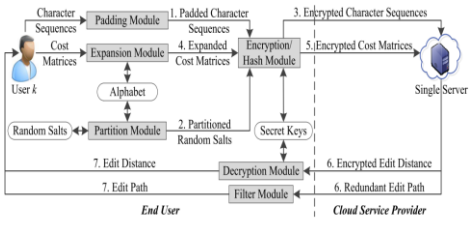
PROPOSED SYSTEM

We have proposed a verbal exchange plan that can provide relaxed key distribution and communication for a dynamic institution. We offer a comfortable manner to distribute keys without any communication channels. Users can securely obtain their private keys from the group supervisor with none CAs verifying the user's public key. Our gadget can provide controlled get admission to in element, through the user organization listing, any user in the group can use the origin within the cloud, and revoked users cannot get admission to the cloud again after being revoked. We offer a comfy communique system that may be covered from malicious assaults. Revoked customers will now not be capable of restore their authentic files once revoked, even supposing they may be colluding with an untrusted cloud. Our layout can offer secure comments to the user with a polynomial function. Our program can efficaciously guide dynamic corporations, when a brand new person joins a set or user, the private keys of different users do not want to be recalculated and updated. We offer a security evaluation to prove the security of our plan.

CONVENIENT PROPOSAL SYSTEM

- Strength of Persuasion and Power
- Greater sure
- Safer and more efficient.
- Data privateness

SYSTEM ARCHITECTURE



CHAPTER IV
Modules

There are Used five Different Modulus

4.2.1 Login Module
4.2.2 Registration Module
4.2.3 Creation Storage and Instance
4.2.4 Find collusion Module
4.2.5 Find Third-Party Module

4.2.1 Login Module

This is the primary motion. The consumer need to provide the suitable touch range and password that the user enters in the registration to go into the software. If the data from the person matches the data within the database, the consumer is efficiently logged into the utility, otherwise a login failure message is displayed and the consumer should re-enter the proper information. A registration link is likewise furnished for brand spanking new consumer registrations.

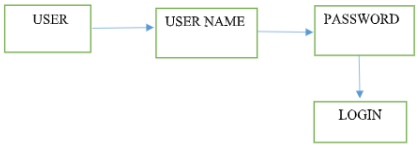


Fig 4.2 Login Module

INPUT: User Name and Password
OUTPUT: Admin Login

4.2.2 Registration Module

A new person who desires to get admission to the utility ought to register earlier than logging in. Clicking the register button in the login movement opens to register the data. A new consumer is registered with the aid of entering their complete call, password and contact range. The consumer need to re-enter the password within the Confirm Password textual content container. When the user enters statistics in all the text fields, while the login button is clicked, the statistics is transferred to the database and the user is directed to login again.

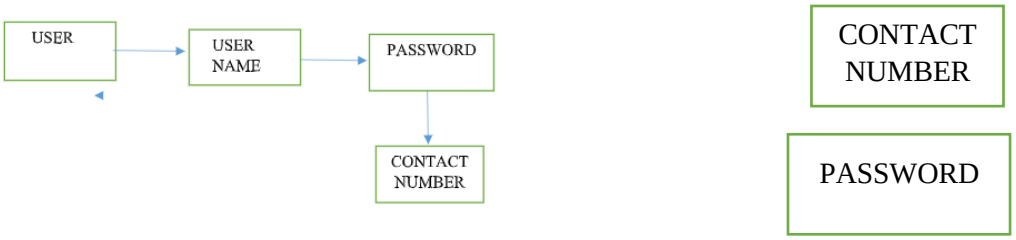


Fig 4.3 Registration Module

**INPUT : ** User Name and Password
OUTPUT: Database

4.2.3 Creation Storage and Instance

The statistics proprietor has no manipulate over the facts once it's far uploaded to the cloud. In this module, the original facts is encrypted in one-of-a-kind values. The statistics in every block may be encrypted using diverse cryptographic algorithms and encryption keys before being saved in the cloud.

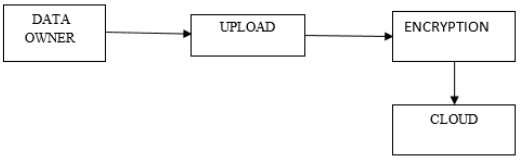


Fig 4.4 Creation Storage and Instance

**INPUT : ** User Name and Password
OUTPUT: data uploaded

4.2.4 Find Collusion Module

In this module, the Receiver can stumble on the presence or absence of collusion by calculating the user's distance.

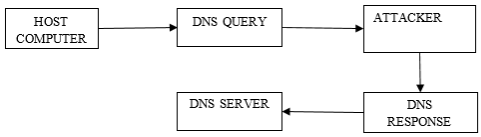


Fig 4.5 Find Collusion Module

INPUT : User Name and Password
OUTPUT: Database

4.2.5 Find Third-Party Module

In this module, the recipient can discover 0.33 events. Third celebration refers to another enterprise that produces the original dealer's software program.

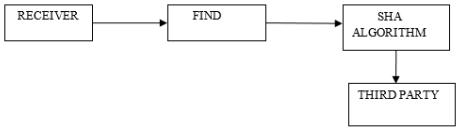


Fig 4.6 Find Third-Party Module

INPUT : User Name and Password
OUTPUT: find third-parties

4.3 Data Flow Diagram

A facts go with the flow diagram (DFD) is a graphical representation of the "go with the flow" of statistics thru an records machine, forming a view of the system. Often, preliminary steps are used to create an outline of the machine, that may then be advanced. DFD can also be used to visualize technique information (structured diagram)

4.3.1 DFD-Level 0: Data Owner

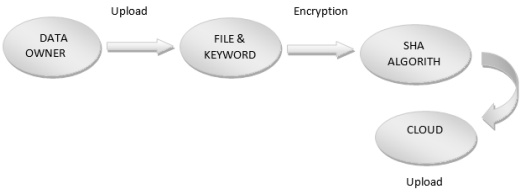


Fig 4.7 DFD-Level 0: Data Owner

4.3.2 DFD-Level 1:

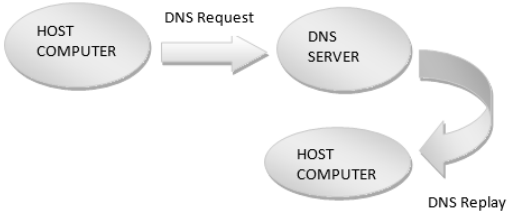


Fig 4.8 DFD-Level 1:

4.3.3 DFD-Level 2:

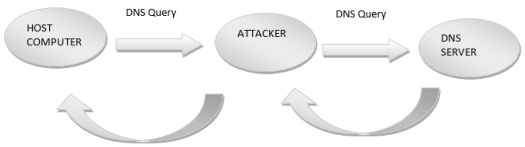


Fig 4.9 DFD-Level 2:

4.4 SYSTEM DIAGRAM

4.4.1 Use case Diagram

A Unified Modeling Language (UML) use case diagram is a form of human diagram described and constituted of use case analysis. The purpose is to provide a graphical evaluate of the functionality of the gadget in phrases of actors, their goals (represented as use cases), and any dependencies between consumer instances.

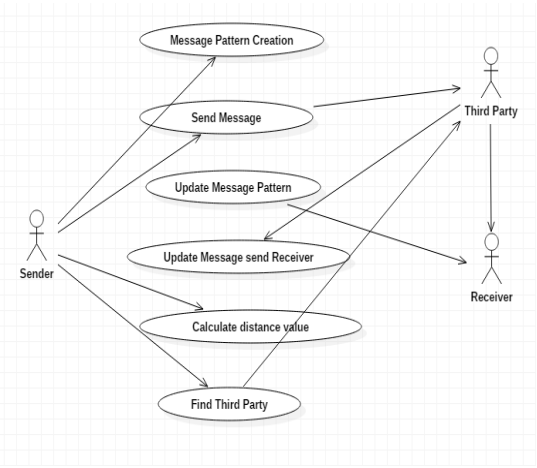


Fig 4.10 Use Case Diagram

4.4.2 Class Diagram

A elegance is the fundamental constructing block of item-oriented modeling. It is used to version the overall concept of a scientific utility and for the expressed models translated into program code.

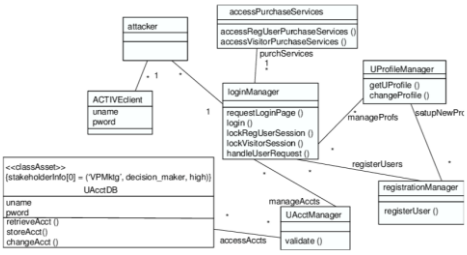


Fig.4.11 Class Diagram

4.4.3 Sequence Diagram

A Unity Connection Language (UML) sequence diagram is a type of interaction diagram that indicates how methods intersect with every other and in what order. This publish is a series of posts. A series diagram is from time to time known as an event diagram and a timing chart.

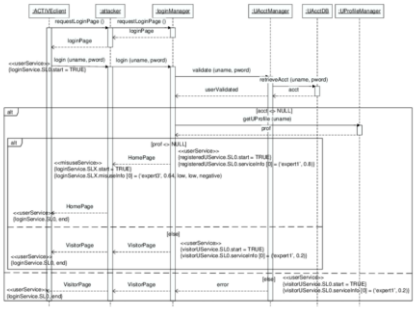


Fig: 4.12 Sequence Diagram

4.4.4 Activity Diagram

Activity diagrams are a graphical illustration of steps and sports based on guide for selection, iteration and concurrency. In a completely unique modeling language, an interest diagram can be used to explain the business and operational steps of the workflow components in a machine. The movement plan shows the redundancy control.

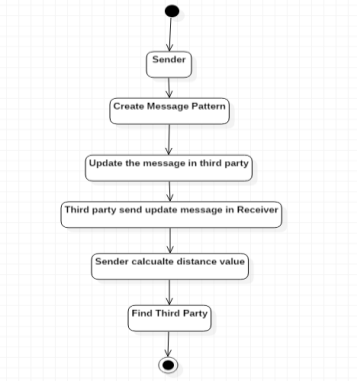


Fig: 4.13 Activity Diagram

4.4.5 Component Diagram

A aspect diagram is designed to visualise the company and relationship between them. Systems are beneficial while constructing an executable device. The person, the user's teacher, and the auditor are the third party executable elements of the machine.

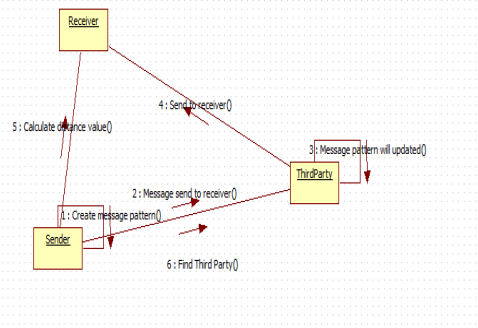


Fig: 4.14 Component Diagram

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- System - Pentium-IV
- Speed - 2.4GHZ
- Hard disk - 40GB
- Monitor - 15VGA color
- RAM - 512MB

SOFTWARE REQUIREMENTS:

Operating System - Windows XP
Coding language - Java
IDE - Net beans
Database -MYSQL

SYSTEN DESIGN

Input Design

The enter method is the link among the statistics gadget and the user. It involves the improvement of a specification and manner for facts coaching, and these steps are essential to carry the transactional records right into a usable process shape, which can be accomplished by means of computer studying the statistics from a written or published script, or this will. It is going to be completed with the help of the humans, introducing the keys. Given without delay into defects. Input planning focuses on controlling the amount of input required, controlling errors, and averting delays, keeping off extra steps, and retaining the technique easy. The login is designed to be safe and comfortable at the same time as preserving user privateness. The committee's input changed into as follows:

- What facts should be supplied for input?
- How is the facts organized or encoded?
- Alternate box to assist personnel input facts.
- Methods of making ready enter validation and taking movements on errors.

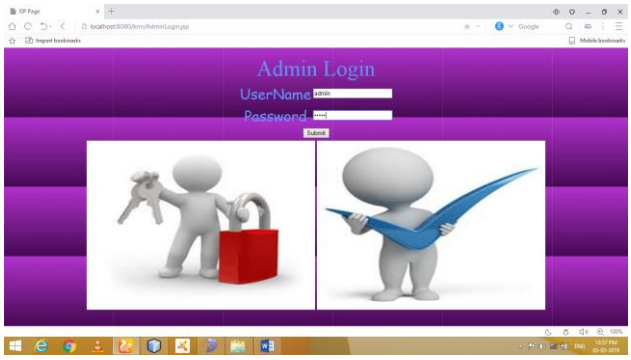
Output Design

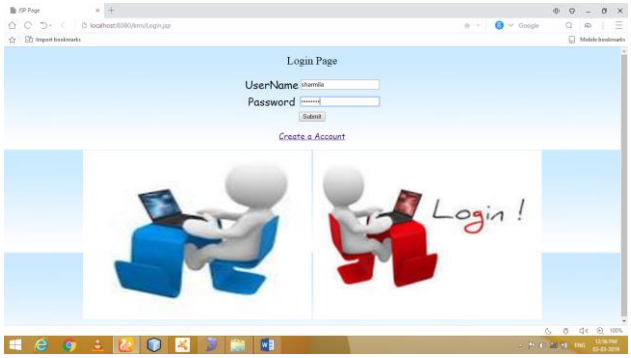
Quality is a end result that meets the cease person's necessities and suggests the statistics absolutely. In any device, the consequences of the system are suggested to customers and other systems through outputs. The output plan defines how records is to be moved for fast need in addition to for printed output. It is the primary and instantaneous supply of statistics for the consumer. Efficient and intelligent output layout of the relationship machine improves, supporting the user to make choices.

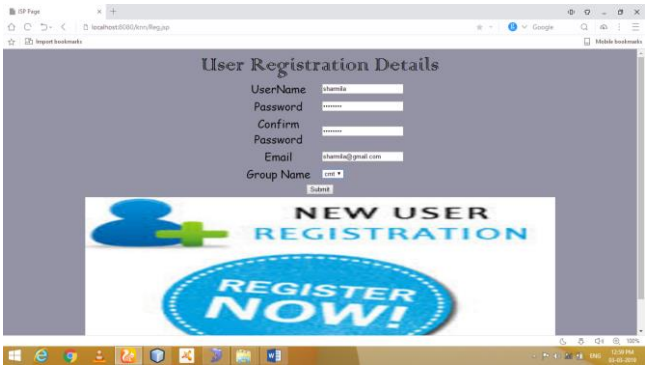
The output format of the records device must perform one or more of the subsequent capabilities.

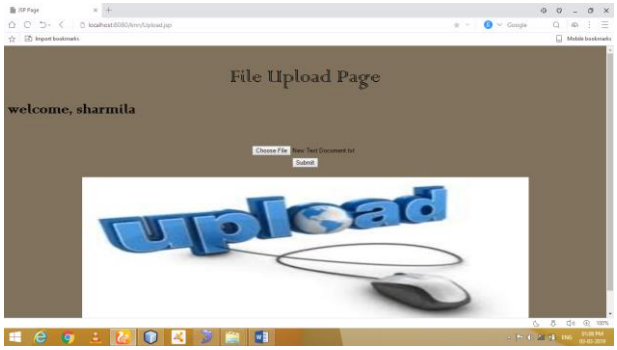
- Communicate statistics approximately beyond sports, cutting-edge status or forecast
- The destiny
- Critical events, opportunities, questions or reminders.
- Lead the action.
- Confirm movement

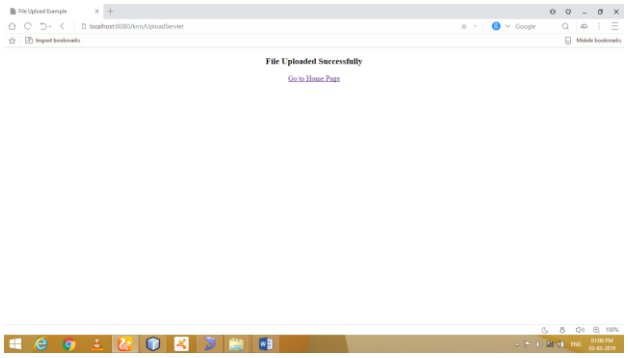
SCREENSHOTS











REFERENCES:

1. Y.Feng,H.Ma,andX.Chen,‘‘Efficient and verifiable outsourcing scheme of sequence comparisons,’’ Intell. Autom. Soft Comput., vol. 21, no. 1, pp. 51–63, Jan. 2015.
2. M. J. Atallah and J. Li, ‘‘Secure outsourcing of sequence comparisons,’’ in Proc. Int. Workshop Privacy Enhancing Technol. (PET), Toronto, ON, Canada, 2004, pp. 63–78.
3. M. J. Atallah, F. Kerschbaum, and W. Du, ‘‘Secure and private sequence comparisons,’’ in Proc. ACM Workshop Privacy Electron. Soc. (WPES), Washington, DC, USA, 2003, pp. 39–44.
4. D. Szajda, M. Pohl, J. Owen, and B. Lawson, ‘‘Toward a practical data privacy scheme for a distributed implementation of the Smith-Waterman genome sequence comparison algorithm,’’ in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA, 2006, pp. 253–265.
5. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, ‘‘New algorithms for secure outsourcing of modular exponentiations,’’ IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.
6. R. Akimana, O. Markowitch, and Y. Roggeman, ‘‘Secure outsourcing of DNA sequences comparisons in a Grid environment,’’ WSEAS Trans. Comput. Res., vol. 2, no. 2, pp. 262–269, Feb. 2007.
7. M. Blanton, M. J. Atallah, K. B. Frikken, and Q. Malluhi, ‘‘Secure and efficient outsourcing of sequence comparisons,’’ in Proc. Eur. Symp. Res. Comput. Secur. (ESORICS), Pisa, Italy, 2012, pp. 505–522.
8. Y. Feng, H. Ma, X. Chen, and H. Zhu, ‘‘Secure and verifiable outsourcing of sequence comparisons,’’ in Proc. Int. Conf. Inf. Commun. Technol. (ICT-EurAsia), Yogyakarta, Indonesia, 2013, pp. 243–252.
9. S. Salinas, X. Chen, J. Li, and P. Li, ‘‘A tutorial on secure outsourcing of large-scale computations for big data,’’ IEEE Access, vol. 4, pp. 1406–1416, Apr. 2016.
10. X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, ‘‘Verifiable computation over large database with incremental updates,’’ IEEE Trans. Comput., vol. 65, no. 10, pp. 3184–3195, Oct. 2016.