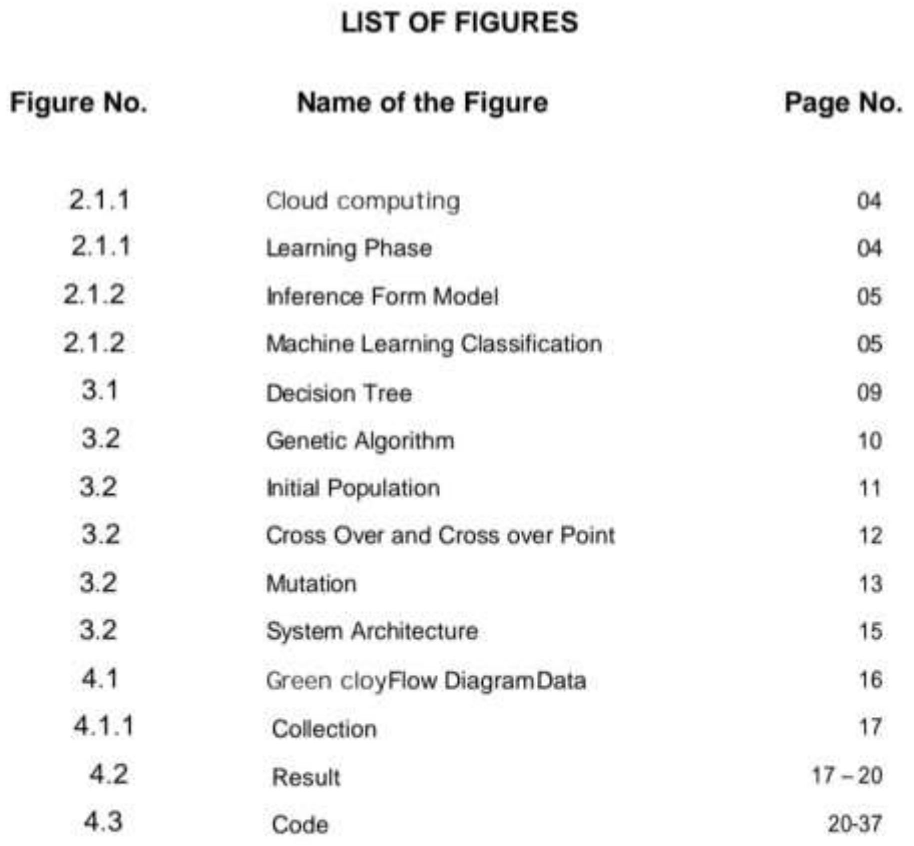
ABSTRACT

Intrusion detection systems (IDSs) are currently drawing a great amount of interest as a key part of system defense. IDSs collect network traffic information from some point on the network or computer system and then use this information to secure the network. To distinguish the activities of the network traffic that the intrusion and normal is very difficult and to need much time consuming. An analyst must review all the data that large and wide to find the sequence of intrusion on the network connection. Therefore, it needs a way that can detect network intrusion to reflect the current network traffics. In this study, a novel method to find intrusion characteristic for IDS using genetic algorithm machine learning of data mining technique was proposed. Method used to generate of rules is classification by Genetic algorithm of decision tree. These rules can determine of intrusion characteristics then to implement in the genetic algorithm as prevention.so that besides detecting the existence of intrusion also can execute by doing deny of intrusion as prevention.

TABLE OF CONTENTS



LIST OF FIGURES

DATA SECURITY IN GREEN CLOUD

ABSTRACT

- Green computing is defined as the study and practice of designing , manufacturing, using, and disposing of computers, servers, and associated subsystems-such as monitors, printers, storage devices, and networking and communications systems-efficiently and effectively with minimal or no impact on the environment."

- Cloud software service is a modality for providing computer facilities and deploying software via the Internet. The concept combines Cloud Computing and Software-as-a-Service (SaaS).
- Cloud computing represents a contextual shift in how computers are provisioned and accessed.
- There are many different examples of cloud software service, and this paper seeks to combine the salient elements into a composite picture of the subject matter.

OBJECTIVE

- The goal of green computing is to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability of outdated products and factory waste.
- Green computing can be achieved by either Product Longevity Resource allocation or Virtualization or Power management.
- Power is the bottleneck of improving the system performance.

AIM

The main aim of this project, Two-Side verification is a process that involves two authentication methods performed one after the other to verify that someone or something requesting access is who or what they are declared to be.

INTRODUCTION

`In recent years, cloud computing technologies have gotten rapid developments and a line of studies have been done on security issues in cloud computing, such as access control and privacy protection. As a typical service in cloud computing, cloud storage needs both data security and search functionality.In fact, user-side verifiability takes into consideration that the cloud server may be malicious, that is, the cloud server may only return part of search results or maliciously return incorrect results. The issue of user-side verifiability is firstly addressed in. However, these two schemes cannot support server-side verifiability and fair payment without any trusted third party. Furthermore, server-side verifiability takes into consideration that the data owner may be malicious, that is, the data owner may maliciously outsource invalid data in the data storage phase and fraudulently claim compensationlater.Thisconcernhasnotbeenaddressedand even has received little attention in the literature. Last but not least, most of the previous schemes are bank-dependent. Specifically, either the payment issue is not considered or the default traditional payment mechanism is exploited in which a trusted third party (TTP) such as a trustworthy bank has to be introduced for payment fairness. Payment fairness can promote the honest behaviors of users and cloud servers [7]. If a malicious behavior is detected based on the user-sideverifiability(resp.server-sideverifiability),thedata owner(resp.cloudserver)shouldgetadequatecompensation from the cloud server (resp. data owner) no matter what the cloudserver(resp.dataowner)does.Therefore,fairpayment without any third party is a meaningful and challenging task and it remains in SSE.

In order to throughly address the aforementioned challenging issues in cloud computing, we propose TKSE, a Trustworthy Keyword Search scheme over Encrypted data without needing any third party. TKSE is proven secure and ourperformanceevaluationshowsitsefficiency.Inparticular, TKSE is characterized by the following desirable features.

- Keyword Search over Encrypted Data. The encrypted data index based on the Elliptic Curve Digital Signature Algorithm(ECDSA)allowsausertosearchovertheoutsourced encrypted data.

- User-side Verifiability. In TKSE, a data owner can embed searchrequirementsintotheoutputscriptofajointtransactionsuchthatthetransactioncanberedeemedbythecloud serverifandonlyiftheoutputscriptevaluatestotruebasedonthereturnedsearchresult.Therefore,TKSEenablesthe data owner to resist malicious cloud servers and user-side verifiability is realized.

- Server-side Verifiability. Similar to user-side verifiability, thepublicverificationofdigitalsignatureenablesthecloud server to check the validness of the outsourced encrypted data from the data owner in the data storage phase. Thus, malicious data owners can be detected by the cloud server, which realizes server-side verifiability.

- Fair Payment and No TTP. Based on hash functions andECDSA, TKSE is compatible with blockchains such as the Bitcoinblockchain and the Ethereumblockchain. The global consensus and distributed nature of a blockchain enable a fair payment mechanism in TKSE without introducing any TTP.

LITERATURE REVIEW

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then the next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

The major part of the project development sector considers and fully survey all the required needs for developing the project. For every project Literature survey is the most important sector in software development process. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

Identity-based encryption with outsourced revocation in cloud computing

Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate. In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

New publicly verifiable databases with efficient updates

The notion of verifiable database (VDB) enables a resource-constrained client to securely outsource a very large database to an untrusted server so that it could later retrieve a database record and update it by assigning a new value. Also, any attempt by the server to tamper with the data will be detected by the client. Very recently, Catalano and Fiore [17] proposed an elegant framework to build efficient VDB that supports public verifiability from a new primitive named vector commitment. In this paper, we point out Catalano-Fiore's VDB framework from vector commitment is vulnerable to the so-called forward automatic update (FAU) attack. Besides, we propose a new VDB framework from vector commitment based on the idea of commitment binding. The construction is not only public verifiable but also secure under the FAU attack. Furthermore, we prove that our construction can achieve the desired security properties.

A searchable symmetric encryption scheme using blockchain

At present, the cloud storage used in searchable symmetric encryption schemes (SSE) is provided in a private way, which cannot be seen as a true cloud. Moreover, the cloud server is thought to be credible, because it always returns the search result to the user, even they are not correct. In order to really resist this malicious adversary and accelerate the usage of the data, it is necessary to store the data on a public chain, which can be seen as a decentralized system. As the increasing amount of the data, the search problem becomes more and more intractable, because there does not exist any effective solution at present. In this paper, we begin by pointing out the importance of storing the data in a public chain. We then innovatively construct a model of SSE using blockchain(SSE-using-BC) and give its security definition to ensure the privacy of the data and improve the search efficiency. According to the size of data, we consider two different cases and propose two corresponding schemes. Lastly, the security and performance analyses show that our scheme is feasible and secure.

BlockchainBased system for secure data storage with private

Key word search

Traditional cloud storage has relied almost exclusively on large storage providers, who act as trusted third parties to transfer and store data. This model poses a number of issues including data availability, high operational cost, and data security. In this paper, we introduce a system that leverages blockchain technology to provide a secure distributed data storage with keyword search service. The system allows the client to upload their data in encrypted form, distributes the data content to cloud nodes and ensures data availability using cryptographic techniques. It also provides the data owner a capability to grant permission for others to search on her data. Finally, the system supports private keyword search over the encrypted dataset.

Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems

Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advices from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. The rapid development of blockchain technology promotes population healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of N from N -1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies.

Existing System

- In slight contrast, it is used and own by an organization internally, anyone within the organization can access the data, services and web application except for outside, reaffirmed the above assertions and added that, a private cloud provides the upmost degree of control over performance, trustworthiness and security.