Secure Transmission by Employing Multi-Biometric Authentication in Cloud Computing

Sarah S and Persi Pamela
Assistant Professor, Department of IT, Kingston Engineering College, Vellore, TamilNadu, India

Abstract—Cloud computing entrusts remote services with a user’s data, software and computation. The basic principles of cloud computing is to make the computing be assigned in a large number of distributed computer system, rather than local computer or remote server. The security of access control systems is enhanced by using various biometric authentication mechanisms to identify the authorized personnel. We propose an orthogonal design and the new authentication framework with pattern recognition algorithm on the network server without any modification of access clients.

Keywords -- Cloud Computing, Orthogonal Design, Biometrics, Access Control, Pattern Recognition

I. INTRODUCTION

The emerging Cloud computing field offers so many advantages to the web connected devices. A layered framework is required to secure the data in cloud. The storage security and the data security is must to store, manage, share, analyze and utilize the substantial amount of data. Data residing on the cloud should be secure, authenticated and encrypted so that three level securities can be provided.

The cloud system should (a) support the efficient and encrypted storage of sensitive data (b) supervise, query and save the enormous amount of data (c) support strong reliability and authentication (d) sturdily maintain integrity and confidentiality of the secret data.

II. TYPES OF CLOUDS

In providing a secure Cloud computing solution, a major decision is to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a public, private and hybrid cloud.

A. Public Cloud

A public cloud is a model which allows users’ access to the cloud via interfaces using mainstream web browsers. It’s typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization.

B. Private Cloud

A private cloud is set up within an organization’s internal enterprise datacenter. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure.

C. Hybrid Cloud

A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet.

![Fig.1 Types of Cloud](image)

III. ACCESS CONTROL METHODS

Access Control allows one application to trust the identity of another application. The traditional model for access control is application-centric access control, where each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures. So cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and entitlement information.

The main types of access control models are,

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control (RBAC)

IV. MANAGING CLOUD COMPUTING SECURITY

Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. Biometric samples include finger prints, retinal scans, face recognition, voice prints and even typing patterns. Biometric authentication in cloud computing, its various techniques and how they are helpful in reducing the security threats are explained in detail in this paper. It provides a comprehensive and structured overview of biometric authentication for enhancing cloud security. The types of biometrics are shown in Fig.2.

In this paper, Finger print recognition and Iris Recognition are taken into consideration for biometric authentication.

A. Finger Prints Recognition

Fingerprint refers to an arrangement of elevations and valleys on the exteriors of the finger whose formation is firm. Finger print recognition refers to the mechanized process of ascertaining the uniqueness of a single centered on the evaluation of two impressions.
B. Iris Recognition

Iris recognition is a technique used to recognize individuals based on unique arrangements in iris. Patterns present in iris are recognizable and are unique to every human. It is used an important biometric recognition technique.

![Fig.2 Types of Biometrics](image)

V. DESIGN OF MULTI-BIOMETRIC AUTHENTICATION

The existing electronic proximity authentication of access control systems is mainly based on the exchange of encoded identification information stored on the access card. The security and integrity of such static and passive authentication mechanisms suffer from problems such as access card loss and unauthorized duplications. We design and implement a dynamic authentication framework with sensory information for the access.

![Figure 3: System Architecture of Cloud Biometric Authentication](image)

When an access card integrated with wireless rechargeable sensors enters the communication range of an access control client, the access card piggybacks its sensory data to conventional identification information and transmits it (i.e., the electronic key) to the access control client. The information received by the access control client is then forwarded to the network server for authentication. If both sensory data and identification match a valid record in the authentication database, the network server then instruments the actuator and grants the card holder the access to the system.

Trusted users can share the cards and predefined actions with each other, which is unavailable in biometric authentication systems. Different from existing authentication methods such as combining RFID and an additional keypad near the reader, we propose an orthogonal design in this paper and the new authentication framework only revises authentication algorithm on the network server without any modification of access clients.

In fact, because we piggyback sensory data to ID information before transmitting them to the reader most existing works on communication encryption for RFID system can be easily adopted into our authentication method and therefore deal with several security vulnerabilities such as replay attack and eavesdropping.

The identification information on access cards normally is static. With the addition of dynamic sensory data from onboard sensors, we are able to significantly increase the security key space P and hence the security level for existing electronic authentication systems. A wide variety of sensors including accelerometer, gyroscope, and so on can be used in our system.

To illustrate the basic concept and the resulting security enhancement of our sensory data enhanced access control system design, we use both three axis accelerometer and gyroscope as examples in the following sections. In particular, we utilize the sensory data generated from the rotation of accelerometer and gyroscope to introduce reference designs for the proposed sensory data enhanced authentication scheme.

VI. PATTERN RECOGNITION ALGORITHM

A biometric system is a pattern recognition system, so it involves pattern recognition as the main discipline, as well as image processing, computer vision, signal processing, speech recognition and machine learning to develop biometric-based authentication systems.

Pattern recognition is a branch of machine learning that focuses on the recognition of patterns and regularities in data. The terms pattern recognition, machine learning, data mining and knowledge discovery in databases (KDD) are hard to separate, as they largely overlap in their scope. In pattern recognition, there may be a higher interest to formalize, explain and visualize the pattern; whereas machine learning traditionally focuses on maximizing the recognition rates.

In machine learning, pattern recognition is the assignment of a label to a given input value. In statistics, discriminate analysis was introduced for this same purpose in 1936. An example of pattern recognition is classification, which attempts to assign each input value to one of a given set of classes (for example, determine whether a given email is "spam" or "non-spam"). However, pattern recognition is a more general problem that encompasses other types of output as well. Other examples are regression, which assigns a real-valued output to each input; sequence labeling, which assigns a class to each member of a sequence of values (for example, part of speech tagging, which assigns a part of speech to each word in an input sentence); and parsing, which assigns a parse tree to an input sentence, describing the syntactic structure of the sentence.

Pattern recognition algorithms generally aim to provide a reasonable answer for all possible inputs and to perform "most likely" matching of the inputs, taking into account their statistical variation. This is opposed to pattern matching algorithms, which look for exact matches in the input with pre-existing patterns. A common example of a pattern-matching algorithm is regular expression matching, which looks for patterns of a given sort in textual data and is included in the search capabilities of many
text editors and word processors. In contrast to pattern recognition, pattern matching is generally not considered a type of machine learning, although pattern-matching algorithms (especially with fairly general, carefully tailored patterns) can sometimes succeed in providing similar-quality output to the sort provided by pattern-recognition algorithms.

Pattern recognition deals with identifying a pattern and confirming it again. In general, a pattern can be a fingerprint image, a handwritten cursive word, a human face, a speech signal, a bar code, or a web page on the Internet.

The individual patterns are often grouped into various categories based on their properties. When the patterns of same properties are grouped together, the resultant group is also a pattern, which is often called a pattern class.

Pattern recognition is the science for observing, distinguishing the patterns of interest, and making correct decisions about the patterns or pattern classes. Thus, a biometric system applies pattern recognition to identify and classify the individuals, by comparing it with the stored templates.

A. Pattern Recognition in Biometrics

The pattern recognition technique conducts the following tasks −

- **Classification** − Identifying handwritten characters, CAPTCHAs, distinguishing humans from computers.
- **Segmentation** − Detecting text regions or face regions in images.
- **Syntactic Pattern Recognition** − Determining how a group of math symbols or operators are related, and how they form a meaningful expression.

The following table highlights the role of pattern recognition in biometrics

<table>
<thead>
<tr>
<th>Pattern Recognition Task</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character Recognition (Signature Recognition)</td>
<td>Optical signals or Strokes</td>
<td>Name of the character</td>
</tr>
<tr>
<td>Speaker Recognition</td>
<td>Voice</td>
<td>Identity of the speaker</td>
</tr>
<tr>
<td>Fingerprint, Facial image, hand geometry image</td>
<td>Image</td>
<td>Identity of the user</td>
</tr>
</tbody>
</table>

B. Components of Pattern Recognition

Pattern recognition technique extracts a random pattern of human trait into a compact digital signature, which can serve as a biological identifier. The biometric systems use pattern recognition techniques to classify the users and identify them separately.

The components of pattern recognition are as follows

VII. SECURING THE TRANSMISSION

The data communication between the client and cloud server passes through the network, where it can be exploited. Malicious flooding routes need to be handled by setting a limit for each route [11]. The number of packets a route can transfer defines its limit. To secure the transmission signals encryption algorithms i.e. public key and private key encryption, can be used with spread spectrum modulation [12]. Wireless transmission can be secured using Wired Equivalent privacy (WEP), SSID for each access point and MAC address filtering.

A. Tunneling

The concept of tunneling can be used to secure the data during transmission. The packet destined for the cloud server can be encapsulated in a packet with the address of a different node. Packets on reaching this node will be redirected to the server by the node. This encapsulation prevents the attacker to track down packets meant for the server thus reducing their possibility of getting hacked. The threat ofoggle hacking can also be reduced by incorporating this methodology.

B. Use of Virtual Circuits

The IP packets are transferred as datagrams through the network, so they follow the best path possible. However, they may pass through the router which may have been attacked by an attacker. In such cases, the packets can be traced down and exploited by the attacker. To prevent this attack a virtual circuit can be implemented. In this methodology, the server during the connection establishment sets a fixed route, which the data packets need to follow. This path is through authorized routers. This path insures data security but may fail if a router on the path is down.

C. Secure Cloud Transmission Protocol (SCTP)

Design In internet, services are accessed through web browser using http’s protocols such as HTTP, HTTPS & S-HTTP. HTTP is an application layer protocol which helps in sending and receiving the information. HTTP is not suitable for sensitive information transaction because it is not a secure protocol.
HTTPS is another protocol designed to provide security. This protocol works in presentation layer in encrypting the sensitive transaction. HTTPS is not effective because, along with message body it also encrypts the message header.

Table No:2: Advantages of the Security Measures for cloud environment

<table>
<thead>
<tr>
<th>Security Measures</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two factor authentication with digital signature and one time password.</td>
<td>Secures system without the need of any extra hardware.</td>
</tr>
<tr>
<td>Replicating storage of hashed data.</td>
<td>Secured data available during failure.</td>
</tr>
<tr>
<td>Authenticating for each write with digital signature</td>
<td>Unique identification of client. Secured write.</td>
</tr>
<tr>
<td>Use of virtual circuit along with IDS</td>
<td>Protect an attack during transmission and detect any attack in the code which reaches the server.</td>
</tr>
</tbody>
</table>

CONCLUSION

In this paper, we propose a multi-biometric authentication with secure access control systems. Different from existing schemes of authentication in access control systems, which mainly based on biometric authentication and generate a random key to every time of authentication to users. Our dynamic authentication method combines sensory information from onboard sensors and conventional static ID information. Two case studies of the multi-biometric authentication are proposed. We theoretically analyze their highly increased key space, which exponentially multiplied dynamic key space in existing authentication methods.

REFERENCES


