RESEARCH ARTICLE OPEN ACCESS

Implementing Iris in the Railway Control Office Application for Secure Saas in Cloud Environment

Dr. K. Meena*, Dr. M. Manimekalai**, R. Raghuraman***
*Former Vice-Chancellor, Bharathidasan University, Trichy, Tamilnadu, India
** Director and Head, Department of Computer Applications, Shrimati Indira Gandhi College, Trichy, India
***Principal, Zonal Railway Training Institute, Southern Railway, Trichy, Tamilnadu, India.

ABSTRACT
Technology plays a vital role in each and every part of the world. In particular "Cloud" computing - a moderately recent term, characterizes the path to develop the advancement in the world of computer science. Further, Cloud provides an affordable environment for its users through different forms of services such as SaaS (Software as a service), PaaS (Platform as a service), and IaaS (Infrastructure as a Service). Cloud computing is also an Internet-based computing where a large pool of systems are connected in private or public networks, and provide dynamically scalable infrastructure for application data as well as file storage. Security of Cloud computing is an evolving sub-domain of network security, computer security and information security. In spite of its advantages, Cloud environment has many security flaws such as loss of important data, data leakage and something related to cloning, resource pooling etc. Security of Cloud Computing is an emerging area for study. It includes several security and privacy issues with challenges and solutions for many security issues of cloud computing. The Control Office Application (COA) is the latest addition to train operations related IT application of Indian Railways. Along with the Freight Operations Information System (FOIS), COA has led to a complete transformation in train operations and facilitates all information on train operations being computer generated. It is this application that feeds the National Train Enquiry System (NTES) which provides passengers with up to date information on train running. COA also provides train operations information to FOIS and ICMS. The objective of the Indian Railways is to further improve the operations by using technological aids that enable quicker data capture and intelligent applications that provide better planning and forecasting tools. To overcome these issues, in Cloud computing, we can use SaaS (software as a service). In this paper, we have proposed a new IRIS algorithm to authenticate the users of COA software in the cloud environment.
Keywords – COA, SaaS, PaaS, IRIS, Authentication

I. INTRODUCTION

In the present era, Cloud computing has become one of the most hyped IT innovation [1]. In the world of modern technology, Cloud computing technology is an innovative concept, which affords great prospects in many domain areas. Cloud computing is a combination of computers and servers that are openly accessible via internet [2]. Cloud computing allows consumers and business people to deploy applications without installation and to access their personal files from any computer with internet facility. Cloud computing endows the mixture of internet based on stipulated services like software, hardware, server, infrastructure and data storage [3]. Now a days, cloud computing has become more popular in the field of technology. To authenticate the official users in cloud computing using IRIS recognition system, we have made assessment of some of the existing authentication formats. Firstly, in cloud computing the conventional username and textual password is used. But this method is considered too simple to hack. Some systems have projected graphical and 3D password but it entails more space and time consuming process on validation.

According to a Gartner Group estimate, SaaS sales in 2010 reached $10 billion, and projected to increase to $12.1 bn in 2011, up by 20.7% from 2010. The Customer Relationship Management (CRM) continues to be the leading market for SaaS [4]. In the earlier published paper titled "A Privacy Preserving Repository for Securing Data across the Cloud", the researchers projected the privacy preserving storage area for acceptance of incorporation of the requirements from clients to share data in the cloud and maintain their privacy, collect and amalgamate the apt data from data sharing services, and return the integration results to users [5].

The universal approach is to deliver the data concept with information and control over data privacy is the stipulation under privacy policies explicit to the data shared [6]. SLA negotiation is also a matter of previous research based in the Grid community [7] and presently widening into the cloud

[8,9]. Within the cloud, the SLA negotiation process grips the creation of a SLA captured by deploying the WS agreement XML standard [10]. In the cloud, the service provider confers SLA on behalf of the user with cloud infrastructure providers. In addition, the process of an assessment of privacy has rebuffed into a separate area of research in the form of Privacy Impact Assessments (PIA) [11]. In 1920's, PIA have emerged from existing work on data access by Organizations to more specific mentions of PIA in terms of technology in the 1970s, wherein a wide range of research has been undertaken [12].

As a result of widespread fragmentation in the SaaS provider space, there is a promising trend towards the advancement of SaaS Integration Platforms (SIP). These SIPs permit the subscribers to employ the multiple SaaS applications through a common platform. In addition, they also offer new-fangled application developers an opportunity in quickly developing the new applications. According to a survey of 600 enterprises by Enterprise Strategy Group 2012 it is stated that the use of SaaS is bound to consistent rise. In terms of the result of the present survey, it is established that 46% of existing users have adopted SaaS, 17% do not use but are planning to use, 21% don not use or plan but were interested to use, 14% do not use, plan or show interest and 1% were not clear [13]. However, the safety is one of the most significant concerns of SaaS. In a survey 51% of the people attributed security as the primary concern where as 40% opined incorporation with other application, 34% lack of customization and 33% total cost of ownership as other possible reasons for not using Saas[14].

II. SECURITY ISSUES OF SAAS IN CLOUD COMPUTING

In Software as a Service (SaaS) model, the customer desires to be reliant on the service provider for proper security measures of the system. The service provider must guarantee that their multiple users don't get to see each other's private data. Subsequently, it becomes more important for the users to make sure that right security measures are in place and also it is not tricky to get an assurance that the application will be available, as and when needed by them [15]. Cloud computing providers have a definite role to solve the common security challenges that a conventional communication systems faces under different situations. At the same time, they should also provide solutions with other issues inherently catered to by the cloud computing paradigm itself.

2.1 Authentication and Authorization

The authorization and authentication applications employed in enterprise backgrounds need to be distorted, so that they can work even under a safe cloud environment. Forensic tasks will become more difficult because it will be very hard or may not be possible for investigators to access the system hardware physically.

2.2 Data Confidentiality

Confidentiality may relate to the hindrance of unintentional or intentional unauthorized disclosure or distribution of secured private information. Confidentiality is strongly related to the areas of encryption, intellectual property rights, traffic analysis, covert channels, and inference in cloud system. Whenever a business, an individual, a government agency, or any other entity wants to distribute the information over cloud, confidentiality or privacy is a big question which needs to be addressed.

2.3 Availability

The availability guarantees reliable and timely access to cloud data or cloud computing resources to the authorized users. The availability is one of the immense concerns of cloud service providers, as cloud service if disrupted or compromised in any way may affect a large no. of customers than in the conventional model.

2.4 Information Security

In the SaaS model, the data of an enterprise is piled up outside the enterprise boundary, which is technically at the SaaS vendor premises. Consequently, the SaaS vendor needs to implement additional security features to ensure data security and thwart breaches due to security vulnerabilities in the application or by malicious employees. This will help us to understand the need for use of strong encryption techniques for data security and highly competent authorization to control access over private data.

2.5 Data Access

Data access issue is primarily associated with security policies afforded to the users while accessing the data. Each and Every Organization have their own security policies based on which their employees can have access to a particular set of data. These security policies must be held on by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be stretchy enough to integrate the specific policies put forward by the organization.

2.6 Network Security

In a SaaS development model, highly sensitive information is obtained from the various enterprises, then processed by the SaaS application and stored at the SaaS vendor's premises. All data flow over the

network has to be secure to facilitate prevention of leakage of sensitive information.

2.7 Data Breaches

Since data from different users and business organizations reside together in a cloud environment, breaching into this environment will potentially make the data of all the users vulnerable. Thus, the cloud serves as a high potential target.

2.8 Identify Management and Sign-on Process

Identity management (IDM) or ID management is the field that enables to identify the individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. The area of IdM is considered as one of the biggest challenges in information security. When a SaaS provider intends to manage the users for access control within the enterprise, it becomes a really mundane task.

III. AUTHENTICATION IN CLOUD

As cloud users store their information through an assortment of services across the Internet, it can be easily accessed by unauthorized people [16]. So security is the most important issue in cloud computing. To provide security, it necessitates proper authentication techniques in cloud computing. Typically, authentication is done based on information about one or more of the following: (i) Knowledge of the subject, such as password or secret information. (ii) Possession of the user, such as smart card, passport, driver's licence, etc. (iii) Biometric traits of the client, such as fingerprint, voice, iris, etc. [17].

The data leakage and security attacks can originate mainly due to insufficient authentication [18]. Cloud services are paid services as a result of which identity of the authorized user becomes a major concern. In this research paper, we focus on the safety measures in cloud computing, more particularly on authentication. To solve authentication problems in cloud computing, there are various traditional as well as biometric techniques as highlighted below which do have some negative aspects as well.

3.1 Traditional Authentication Scheme

1) Password – A login id and a password combination is the most commonly used method of authentication but not well secured [19]. It is very easy to hack the password by various tools. 2) OTP – OTP is a One Time Password wherein password is provided upon request. An OTP can thwart a password from being stolen and reused [20]. This password is valid for a limited period of time (say 5 minutes) and can be used only once. This kind of an authentication is fairly expensive.

3.2 Biometrics Authentication Techniques

1) However, Now-a-days, Biometrics is one of the most extensively used security system. It helps to overcome a lot of drawbacks of above stated techniques of authentication. Biometrics can be defined as an automated methodology in exceptionally identifying the humans by their behavioural or physiological characteristics [21].
2) There are several biometric techniques as listed below:
3) Voice Recognition – As the name suggests voice recognition involves authentication with respect to vocal data. Voice recognition is used to authenticate user's identity based on patterns of voice pitch and speech style. But a user's voice can be easily recorded and may be used by an unauthorized user. Also voice of a user may change due to sickness, which makes identification difficult.
4) Signature Recognition – Signature recognition is used to authenticate user's identity based on the traits of their unique signature. People may not always sign in a consistent manner and hence verifying an authorized user is difficult.
5) Retinal Recognition – Retinal recognition is for identifying people by the pattern of blood vessels on the retina. But this technique is very intrusive and expensive.
6) Iris Recognition – Iris recognition is a method of identifying people based on unique patterns within the ring-shaped region surrounding the pupil of the eye. As in the case of retina, this technique is also intrusive and expensive.
7) Fingerprint Recognition – Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. The dryness of fingers, soiled fingers etc. can affect the system and may show an error.
8) Hand Geometry Recognition – Hand Geometry biometrics is based on the geometric shape of the hand. It includes the size of the palm, length and width of the fingers etc. But this technique has some drawbacks like it is not ideal for children as with increasing age their hand geometry tends to change and also constant use of jewellery may result in change in hand geometry. This technique is not valid for persons suffering from arthritis, since they would not be able to put the hand on the scanner properly.
9) Palm recognition – Palm recognition is based on ridges, principal lines and wrinkles on the surface of the palm. This technique is very expensive and not appropriate for children as

their lines of palm change drastically once they are fully grown up.

IV. IMPLEMENTING PROPOSED IRIS ALGORITHM IN CONTROL OFFICE APPLICATION

In the proposed algorithm, the following steps will take place: Pre-processing, Feature Extraction and Feature Classification.

4.1 Pre-Processing

In this first step, the following processes would take place. Gray scale conversion, Median Filtering, Pupil Center Detection, Canny Edge Detection, IRIS Radius Detection, IRIS Localization, IRIS Unrolling.

4.1.1 Gray Scale Conversion

In this step, the given image with the kernel radius 'r' and size 'm x n' is converted into image of size 'm x n'.
Input: Image X of size m n, kernel radius r.
Output: Image Y of size m x n.
Step 1: Read the image.
Step 2: Convert the image into m x n matrix of pixels
Step 3: For each pixels in both row and column, apply gray scale conversion formula of dividing the RGB value of each pixel by 3.

4.1.2 Median Filtering

Input: Image X of size m n, kernel radius r.
Output: Image Y of size m x n.
Step 1: Initialize each column histogram h0; : : : ; hn1 as if centred on row 1.
Step 2: for i = 1 to m do
Step 3: Shift the rst r column histograms h0; : : : ; hr1 down 1 pixel.
Step 4: Combine these r column histograms to form the kernel histogram H.
Step 5: for j = 1 to n do
Step 6: Set pixel Yi;j equal to the median of H.
Step 7: Remove column histogram hjr1.
Step 8: Add column histogram hj+r.
Step 9: end for
Step 10: end for

4.1.3 Pupil Center Detection

Input: Image X of size m x n.
Output: Image Y of size m x n.
Step 1: **S**can through the median image from top left to bottom right and make no assumptions about the position of the pupil (or eye for that matter).
Step 2: The algorithm begins by finding a pixel that is below the threshold (a combination of the lowest intensity in the current image and some variance)
Step 3: Find the amount of pixels adjacent to the right that has intensity below the threshold as well.
Step 4: This amount is called the block size. The centre of the block is the suspected centre of the pupil.
Step 5: If this block is the largest observed so far, it determines if a block of pixels going in the vertical direction up and down from the center of the block (Effectively making a cross) are also below the threshold and have some variance.
Step 6: If so, the maximum block size is updated and the centre to return is reset to new centre.

4.1.4 Canny Edge Detection

Using the canny edge detection,
Step 1: Detects the edges of the image based on the current threshold and sigma values.
Step 2: The canny edge detector will generate a binary image (black and white) that shows the edges of the image.
Step 3: This image is saved into the subject as the edge image.

4.1.5 Pupil/ IRIS Radius Detection

If the percentage of the pixels along the circle defined by the current radius and the pupil centre that are black is greater than the given threshold percentage, the iris has been found.

4.1.6 IRIS Localization

1) The radius identified by the pupil center detection and finds a radius for which the circle in the edge image has at least a certain amount of black pixels (edges) on or nearly on the circle.
2) If the proportion of the iris radius meeting this criterion is between two bounds then the iris radius is successfully found.

4.1.7 IRIS Unrolling

1) Unrolls the iris of the subject, defined as the area between the pupil radius and the iris radius.
2) The iris, a circular object is transformed universally into a rectangular image that counteracts the distortion of the wrapping of the iris around the eye.

4.2 Feature Extraction (Extracting a 8*12 Iris Pattern from Edge Detected IRIS Image)

1. Take the 8-Bit BMP Image produced from previous Algorithm as Input and open this BMP file in binary Read Mode.
2. Read the raster Data and Store the raster Data into a Matrix of vector size. Where vector Size = file size - (54+(4*256)).
3. Then a 8*12 Iris Pattern is extracted from Edge Detected BMP using following logic-
for (x=0;x<=originalImage.rows-1;x++) {

```
for (y=0;y<=originalImage.cols-1;y++) {
if ( y < 30 && x = (original Image.rows/2)+4) && Gray Value = =255) {
for (i=0;i<8;i++){
for (j=0;j<12;j++){
*(edgeImage.data + (i * edgeImage.cols) + j) = *(originalImage.data + (x * originalImage.cols) - (i * originalImage.cols) + (y + j));
Write to new BMP Image file
}
}
}
}
}
```

Take 8-bit BMP image produced from previous step as an input. Then convert it to 12X8 8-bit BMP image by following this algorithm. This 12x8 8-bit BMP image is the output of the algorithm. In this algorithm, first go to the middle row and first column of the input image, then go to the 4 pixels upward and check the gray value of each pixel until gray value becomes 255 (white). After this start reading the pixels and store the corresponding gray value into a 8x12 matrix.

V. RESULTS AND DISCUSSIONS

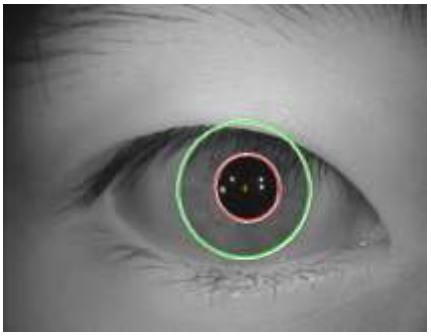

Figure 1: Iris boundaries seem to be perfect circles

In the figure 1, The recognition quality can still be improved if boundaries are found more precisely. Note these slight imperfections when compared to perfect circular white contours.

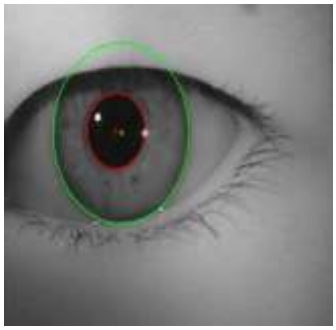

Figure 2: The centers of the iris inner and outer boundaries are different

In the figure 2, the iris inner boundary and its center are marked in red, the iris outer boundary and its center are marked in green.

Figure 3: Gazing-Away Eyes

Figure 3 represents the gazing away eyes are correctly detected on images, segmented and transformed as if it were looking directly into the camera. And in the figure 4, the iris boundaries are not circles and not even ellipse and it is especially in gazing-away eyes.

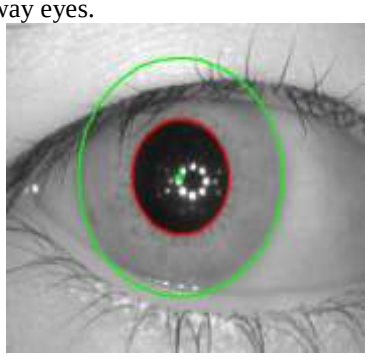

Figure 4: Iris boundaries are definitely not circles and even not ellipses

VI. CONCLUSION

The Control Office Application (COA) is the latest addition to train operations related IT applications. The software of COA for railway department is to be implemented on the cloud environment. Clouds offer the opportunity to build data observatories with data, software and expertise together to solve problems such as those associated with economic modeling, climate change, terrorism, healthcare and epidemics etc. In an emerging discipline, like cloud computing, security needs to be analyzed more frequently. With advancement in cloud technologies and increasing number of cloud users, data security dimensions will continuously increase. For the secure accessing of COA software in the cloud, in this paper, we are introducing a new iris detection algorithm for preventing unauthorized access to the software. Using this algorithm, the recognition quality can still be improved if boundaries are found more precisely and it detects the eyes when the centre of the outer and inner boundaries are different, the gazing away eyes are also correctly detected, segmented and transformed

as if it were looking directly into the camera. And this algorithm helps to improve the security issues in the cloud environment, when the COA software is implemented as a software as a service in the cloud.

REFERENCES

[1] Rajesh Piplode and Umesh Kumar Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume-2, Issue-9, September 2012.

[2] P. Senthil, N. Boopal and R.Vanathi, "Improving the Security of Cloud Computing using Trusted Computing Technology," International Journal of Modern Engineering Research (IJMER), ISSN: 2249-6645, Volume-2, Issue-1, Jan-Feb 2012, pp-320-325.

[3] Ganesh V. Gujar, Shubhangi Sapkal and Mahesh V. Korade, "STEP-2 User Authentication for Cloud Computing," International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume-2, Issue-10, April 2013.

[4] McHall, Tom (7 July 2011). "Gartner Says Worldwide Software as a Service Revenue Is Forecast to Grow 21 Percent in 2011". Gartner.com. Gartner. Retrieved 28 July 2011.

[5] Ranjita Mishra, Sanjit Kumar Dash, Debi Prasad Mishra, Animesh Tripathy "A Privacy Preserving Repository for Securing Data across the Cloud," Proc. Electronics Computer Technology (ICECT), 2011 3rd International Conference , pp. 6-10, 2011.

[6] J. Karat, C.-M. Karat, C. Brodie, and J. Feng. Privacy in information technology: Designing to enable privacy policy management in organizations. Int. Journal of Human-Computer Studies, 63(1-2):153–174 2005.

[7] Hasselmeyer P, Qu C, Schubert L, Koller B, Wieder P. Towards autonomous brokered SLA negotiation. Proceedings of the 2006 eChallenges Conference—Exploiting the Knowledge Economy—Issues, Applications, Case Studies, Cunningham P, Cunningham M (eds.), vol. 3. IOS Press: Amsterdam, 2006.

[8] Rochwerger B, Galis A, Levy E, Caceres J, Breitgand D, Wolfsthal Y, IM Llorente MW, Montero R, Elmroth "E. RESERVOIR: Management technologies and requirements for next generation service oriented infrastructures." Proceedings of the 11th IFIP/IEEE International Symposium on Integrated Management, New York, U.S.A.,2009.

[9] Contract based e-Business System Engineering for Robust, Verifiable Cross-organisational Business Applications (CONTRACT), 2009.

[10] WS-Aggrement-Negotiation v 1.0 2011 http://www.gridforum.org/Public_Comment_Docs/Documents/2011 03/WSAgreementNegotiation+v1.0.pdf.

[11] R. Clarke, Privacy Impact Assessments February 1998, http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html.

[12] R. Clarke. Privacy impact assessment: Its origins and development. Computer Law & Security Review, 25 (2009).

[13] Keep SaaS secure from the start, http://h30458.www3.hp.com/us/us/discover-performance/security-leaders/2012/jun/enterprise-saas-security-issues--concerns--threats---risks---hp-.html.

[14] 5 problems with SaaS security, http://www.networkworld.com/news/2010/092710-software-as-service-security.html.

[15] Choudhary V.(2007). Software as a service: implications for investment in software development. In: International conference on system sciences, 2007, p. 209.

[16] R. Kalaichelvi Chandrahasan, S Shanmuga Priya and Dr. L. Arockiam, "Research Challenges and Security Issues in Cloud Computing," International Journal of Computational Intelligence and Information Security, Volume-3, No-3, March 2012.

[17] Minhaz Fahim Zibran, "Biometric Authentication: The Security Issues," University of Saskatchewan, 2012.

[18] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), Volume-3, Issue-5, 2011.

[19] Maninder Singh and Sarbjeet Singh, "Design and Implementation of Multi-tier Authentication Scheme in Cloud," International Journal of Computer Science Issues (IJCSI), ISSN: 1694-0814 Volume-9, Issue-5, No-2, Sep. 2012.

[20] Aviel D. Rubin Bellcore, "Independent One-Time Passwords," Fifth USENIX UNIX Security Symposium, Salt Lake City, Utah, Jun. 1995.

[21] Chunming Rong and Hongbing Cheng, "A Secure Data Access Mechanism for Cloud Tenants," Cloud computing 2012: The Third International Conference on Cloud Computing, GRIDs, and Virtualization, ISBN: 978-1-61208-216-5, IARIA, 2012.