Multimodal Biometric Authentication to Enhance Security on Cloud

Dr. Nidhi Srivastava,
Assistant Professor
Amity Institute of Information Technology,
Amity University, Lucknow, India

Abstract : Security of data plays a key role in any technology. Cloud computing helps the user in managing the data easily and at low cost. Traditional methods of securing data like password, smart card etc. are not very secure and can be hacked easily. Biometrics of any person is unique and can be used for securing data. In fact, the advantage of using biometrics is that it cannot be forged, forgotten, misused or misplaced. In this paper I have described about cloud computing, security issues with cloud computing and the role biometrics play in securing data in cloud. In this I have given a framework for securing data on cloud using multimodal biometrics and the two modalities used are voice recognition and face recognition. Only if the person is verified then access to the cloud services is given to them.

IndexTerms - Cloud, Biometrics, Unimodal, Multimodal, Voice recognition, Face recognition, Security.

I. INTRODUCTION

With the advent of the Internet and its wide usage more and more people is using it. The personal and professional data is being kept on the cloud now and accessed from there. Keeping the data in cloud has many benefits like low cost, easy maintenance, scalability of resources, etc. But, although cloud offers all good features but security of the data in cloud is a source of concern. Many techniques have been used for securing the privacy of the data, but with one or the other disadvantage. Biometrics of an individual is unique in nature and cannot be copied by anyone. In this paper, I have discussed how multimodal biometrics can be used to secure data in the cloud. Section II of the paper gives an introduction of the cloud computing, its definition and various service and deployment models used in cloud. Section III lists the various security issues in the cloud computing. Section IV gives the benefits of biometrics over traditional security methods; Section V gives a general model of the biometric system. Section VI lists the advantages of multimodal biometrics over unimodal biometric system. Section VII gives the proposed framework for multimodal biometrics on cloud and Section VIII shows the related work done in this area by previous researchers. Lastly, section IX gives the conclusion.

II. CLOUD COMPUTING

The needs in the business organizations are changing at a rapid speed and to keep up with the pace, cloud computing offers decent solution. Cloud computing has fully changed the way IT resources are nowadays being employed and consumed. Cloud computing is being employed today by many organizations like IBM, Google, Amazon, etc. Cloud computing has been defined in various ways.

Cisco [1] defines cloud computing as follows:

"IT resources and services that are abstracted from the underlying infrastructure and provided 'on-demand' and 'at scale' in a multitenant environment."

According to National Institute of Standards and Technology, USA (NIST):

"Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing helps in giving on demand, scalable IT services which can very easily be availed. Some of the advantages of using cloud computing are:

Rapid Elasticity - As per the requirement of the customer features can be elastically increased or decreased.

On demand service – When required the customer can easily access the resources like server, storage, network, etc. Whatever resource is required by the customer they can easily get it.

Measured Service – The resources are controlled and optimized by the cloud provider depending on the service need of the customer. There is full transparency and the customers can easily see the resources used by them.

Resource Pooling – Different resources like memory, processing, storage and network bandwidth, etc. can be dynamically pooled in for the customers as per their requirement. This has the advantage that the customer remains unaware of the location of the various resources being used by them.

Pervasive network access – Through standard mechanism the customer can access all the facilities available on the net.[2, 3, 4]

There are different deployment models of cloud. These are as follows:

Private cloud- It is used in an organization by the users working in that organization. The cloud infrastructure is implemented within the organization by internal IT team of the organization or by any external agency. That is why it is also known as internal or corporate cloud.
Public cloud- This can be accessed by anyone from the public be it an organization, individual or any institution. It is easy to use, inexpensive and security is given so that there is no loss of data.
Community cloud –In this, a specific community with shared concerns like mission, compliance etc. use this cloud. The community may itself comprise of many organizations but all with same vested interest. The cloud may be on-premise or off-premise.
Hybrid cloud- In this the best services of the above mentioned clouds i.e. Public, private and community clouds are taken according to the use of the organizations or institutions. [3,4,5]
There are different service models in cloud. They are
IAAS - In Infrastructure as a service model, the storage, network, server and compute is provided to the consumer on a pay-as-you-go basis. The provider of the cloud mainly controls the above services but consumer can control only the application, operating system and database services.
PAAS – In platform as a service model the customers as per their requirement can use the services and features according to their need. IT resources which are already deployed and configured are available on the Internet and the customers can use the tools provided to improve on their own services and applications. In this the networks, storage, compute, operating system, database, etc. are all on the cloud and the customer keeps the application with himself.
SAAS – In Software as a service model all the resources are managed by the cloud provider and the consumer according to its need uses it. The advantage of this model is that expensive licensed software is easily available in this model and is very cost-effective also. [4, 6, 7]

III. SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing is being used more and more by the organizations and institutions and so the risk of data theft from cloud is also increasing. Cloud service providers provide different cloud services as IAAS, PAAS and SAAS, but each of these has some associated security issues. Sensitive data stored on the cloud can be stolen by the hackers and malicious intruders. Multi-tenancy is the major problem in this. Multi-tenancy means that various consumers share the same resources like memory, network, storage etc. on the same cloud. This may result in the loss of confidentiality of the data and the loss or leakage of important information of the consumer. The user is dependent on the provider to secure their data and if the cloud service providers do not pay much attention or take proper measures then it will lead to breach of data. The applications used in cloud computing are delivered through internet. Hackers can easily take advantage of the flaws in web applications and steal the data. The cloud providers sometimes in turn employ third party on contract basis as service providers for better service. But this may lead to compromise of the confidential data stored. The services on cloud are elastic in nature and so scalable. Due to this scalability, the same resource used by some other customer is allotted to some other customer and this may lead to confidentiality issues. Any organization just accesses the cloud services of any cloud service providers. The organization or the individual has no idea about the employees hired by the cloud providers for doing the work. These cloud employees have full access to the data and thus an insider can be a hacker. Threats from the outsiders also are a cause of concern as it defames the organization and thus can cause reputation, financial and customer loss. The organizations do not know the location of their data which has been ported to the cloud. They do not even know if proper security measures have been taken by the cloud providers or not. Although the cloud providers give username and password access to the customers but it can be easily hacked.[8,9,10]

IV. BIOMETRIC SECURITY VS TRADITIONAL SECURITY MEASURES

The traditional way of safeguarding the data through passwords, pin, smart cards, etc. are not very reliable way of securing data in cloud. For each and every account and different transactions the users need to remember different password. For ease of remembrance, generally the users use the same password for all transactions. But this is very vulnerable because if the hacker gets this one password the hacker can easily access all the accounts of that person. If otherwise the user uses different passwords then remembering each password is a lot difficult for every person. So as not to lose the passwords, if the user stores them at one place then this data is also very much at risk. So the hacker or the malicious user can easily access the data stored in the cloud also. In this case biometrics can play a very significant role.
There are different traits of a person which are unique for each individual. Biometric technology basically deals with these biological traits of the person and extracts the unique features of the traits. There are two types of biometrics methods-physiological and behavioral. Physiological biometrics depends on the physical trait of a person. In this measurement of a part of the human body is taken. Important physiological biometrics include iris-scan, face recognition, fingerprint, retina-scan, palm print, hand geometry and ear recognition. Behavioral biometrics is based on measurements and data derived from an action, and indirectly measure characteristics of the human body. These include signature-scan, voice recognition, keystroke-scan, typing behavior and body odor.[11]
For any of the above trait to be qualified as biometric trait, it should satisfy the requirement of universality, distinctiveness, permanence, collectability, acceptability, performance. Nowadays the biometrics is being used almost everywhere and in every field. Different biometric traits are being used in the organizations. For example for the attendance of the employees, fingerprint scanning is used. For AADHAAR verification iris data is also stored. [12, 13, 14]

V. BIOMETRIC SYSTEM

Some of the research done in the biometrics is especially on finger print, iris and facial recognition. In any of the biometric system there are two important parts: registration and verification or matching. In the registration phase the biometric trait of the person is enrolled. The biometric feature of the person is extracted, normalized and stored in the database for further use. Whereas in the verification phase, the biometric feature of the person is extracted, normalized and matched with the already stored features in the database. If the same matching is made the person is identified. The general model of biometric system is shown in figure 1. [15, 16]

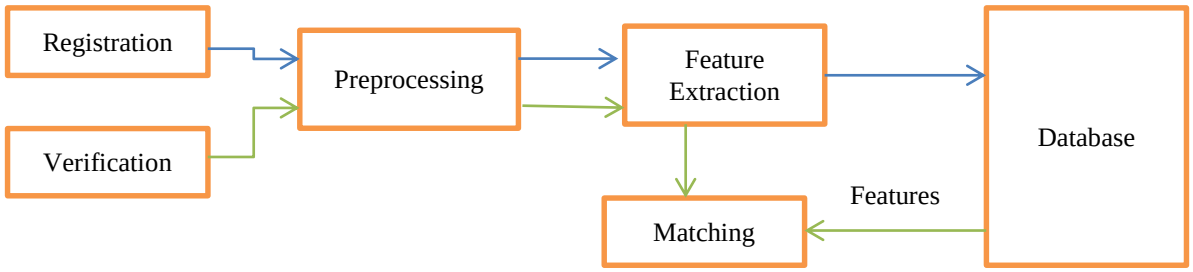

Figure 1: Biometric System

UNIMODAL AND MULTIMODAL BIOMETRICS

Different biometric traits can be used for securing data in the cloud. Various biometrics have different advantages and disadvantages Fingerprint is considered a good biometric method. It is easy to record the data but it is prone to cut and damage and in such a case will not work. Retina and iris scans are very reliable and the storage space required by the features is also very low. But the eyes have to be exposed to light and sometimes the users are not very comfortable with it. Also expensive hardware is required for reading the data. Facial recognition is being very widely used as it can be easily captured through a camera without even the person being aware of it. The only problem with this biometric is that the changing facial expressions of a person make it difficult to recognize the person at times. Voice recognition can also be easily captured and used as a biometric trait. The hardware requirement for this is very easily available and also very cheap. But this will not work in case of sore throat. Also if the background contains lots of noise then identifying the real voice is problematic. Thus using the biometrics over the traditional methods of securing data scores well. But using unimodal biometric systems have many disadvantages like noise creeps into the data, spoofing, non-universality, interclass variations and unreliability. Further, the voice of any particular person can be imitated, the signatures can be easily forged or finger prints can be manipulated, etc. Thus using multimodal biometrics is better. Using more than one biometrics will make the system all the more safe and secure and impenetrable. [15,16]

VI. FRAMEWORK FOR MULTIMODAL BIOMETRICS ON CLOUD

The fusion of any of the above listed modalities can be done for securing data. In this paper, I have used the voice and face modalities for biometric authentication. Acquisition of voice and face data is very easy as the hardware and software needed for both the cases is very easily available and is also very cheap. The data from both the modalities can be fused together for perfect identification of the individual. Fig. 2 shows the proposed architecture. Firstly, the features of both the modalities are extracted and through fusion techniques it is fused. For extraction of the features of the modalities and the fusion different techniques can be used. First the registration of the users is done and their fused biometrics is stored in the cloud for biometrics. Now, whenever the user has to use the cloud service first a verification of the user will be done by matching his biometrics with the stored biometric details. If it is successful, then the user can access the services on the cloud else the access is denied. This is done not only for the customers but also the third party or whoever accesses the data in cloud.

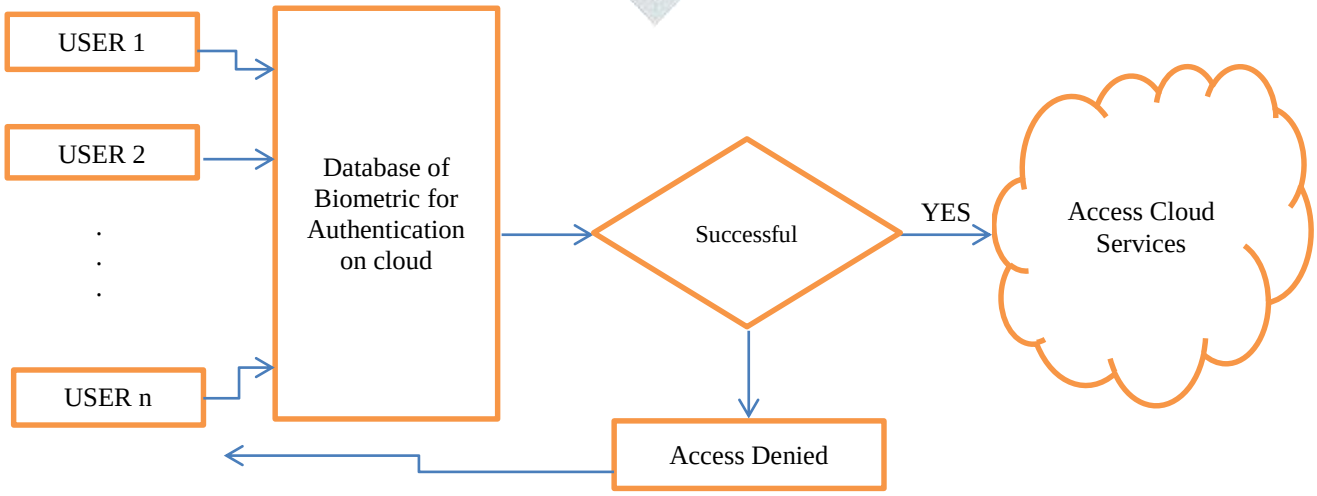

Figure 2: Framework for Multimodal Biometrics security

VII. RELATED WORK

Using biometrics for securing data is being used since very long. But, using the same on cloud has now gained importance. Initially only one modality was emphasized on but now using more than one modality i.e. using multimodal biometrics have gained significance. Some of the research work done in this area has been stated below.

In [10], the authors have told that how the biometrics can be integrated in the cloud services and has also given a case study by implementing the fingerprinting scan along with the password for safe accessing of MODDLE.

In [18] the authors have given a hybrid multimodal biometric method using finger prints and voice biometric method. They have fused and then encrypted the data and then use this for authentication of the user in the cloud.

In [19] the authors have used and implemented fingerprint authentication mechanism on mobile cloud computing. For this the authors have proposed to use the camera of the mobile phone so as to capture the fingerprint images of mobile users.

In [20] the authors have evaluated different strategies of unimodal biometrics which can be combined to give multimodal biometrics. The authors have emphasized on importance of face recognition and fingerprint recognition and then shown that the two together can be used for better security.

In [21] the authors have used iris and fingerprint for data encryption and decryption for security of the data in cloud.

In [22] the authors have used iris, fingerprint and palm print to generate secure biometric key. The results show that this technique is very secure and reliable.

VIII. CONCLUSION

Cloud computing is a good way of accessing and storing data in a flexible manner with reduced cost. Data stored on the cloud can be made secure by using biometrics. In this paper, I have shown the different biometric traits available, their advantages and disadvantages and how multimodal biometrics is more secure over unimodal biometrics. I have also given a framework for using multimodal biometrics in cloud and for securing data in cloud. In future more work on different other multimodal biometrics can be done. Although the challenge remains to collect the biometric traits of a person effectively and without noise.

REFERENCES

[1] Cisco Systems, Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions Point of View White Paper for U.S. Public Sector,, 2009

[2] Tuncay Ercana, Effective use of cloud computing in educational institutions, Procedia, Social & Behavioural Sciences, 2010.

[3] Kalpana N. Meher, Prof. P. S. Lokhande, Cloud Computing: An Architecture, its Security Issues & Attacks, IJARCET, Vol. 2 No. 3, March 2013

[4] Sabuiljjad Hashemi, Cloud Computing Technology For Egovernment Architecture, IJFCST, Vol. 3, No. 6, Nov. 2013

[5] Ganesh Olekar,Vikram Sreekumar, Cloud Computing: Migration from Traditional Systems to the Cloud, IJARCET, Vol. 2 No. 3, March 2013

[6] Nandini Mishra , Kanchan khushwha , Ritu chasta, Abhishek Choudhary, Technologies of Cloud Computing-Architecture Concepts based on Security and its Challenges, IJARCET, Vol. 2 No. 3, March 2013

[7] Dr. Nidhi Srivastava, Effective e-governance through Cloud Computing, IJIRCCE, Vol. 4, No. 3, March 2016

[8] Emerging Security Challenges in Cloud Computing An insight to Cloud security challenges and their mitigation, Akhil Behl, World Congress on Information and Communication Technologies, 2011

[9] Hashizume k., Rosado, D.G.Fernandez-Medina, An analysis of security issues for cloud computing, Journal of Internet Services & Applications, Dec. 2013

[10] Peter Peer, Jernej Bule, J.Z.Gros, Vitomir Strue , Building Cloud-based Biometric Services, Informatica, pp 115-122, January 2013.

[11] P.Padma, Dr. S.Srinivasan, A survey on Biometric Based Authentication in cloud computing, ICICT, IEEE, August 2016.

[12] R.Parkavi, K.R. Chandeesh Babu, J.Ajeeth Kumar, Multimodal Biometrics for User Authentication, 11th International Conference on Intelligent Systems and Control, 2017

[13] Ashish Mishra, Multimodal Biometrics it is: Need for Future Systems, IJCA, Vol. 3, No. 4, June 2010

[14] P.Selvarani, N. Malarvizhi, To Enhance the Data Security in Cloud Computing Using Multimodal Biometric System, World wide journal of multidisciplinary research and development, Vol. 3 No. 7, pp196-201.

[15] P. S. Sanjekar, J. B. Patil, An Overview Of Multimodal Biometrics, SIPIJ, Vol. 4, No. 1, Feb 2013

[16] Mohamed Deriche, Trends and Challenges in Mono and Multi Biometrics, Workshop on IPTA, IEEE, 2008

[17] R. Batool, G. Naveed, A. Khan, Biometric Authentication in Cloud Computing, IJCA, Vol. 129, No. 11, Nov. 2015

[18] Himabindu Vallabhu, R V Satyanarayana , Biometric Authentication as a Service on Cloud:Novel Solution, IJSCE, Vol. 4, No. 2, Sep. 2012.

[19] IehabALRassan, HananAlShaher, Securing Mobile Cloud Using Finger Print Authentication, IJNSA, Vol. 5, No. 6, Nov. 2013.

[20] Z. Emersic, J. Bule, J.Zganec-Gros, V. Struc, P. Peer, A case study on multi-modal biometrics in the cloud, Electrotechnical ReviewVol. 81, No. 3, May 2014

[21] P. Selvarani, N. Malarvizhi, Data Security in Cloud using Multi Modal Biocryptographic Authentication, IJST, Vol. 9, No. 34, Sep. 2016

[22] Teena Joseph, Latha Parthiban, Multimodal biometric based authentication for ensuring data security in Cloud Computing, Journal of Chemical & Pharmaceutical Sciences, Vol. 9, No. 4, Dec. 2016