Biometrics

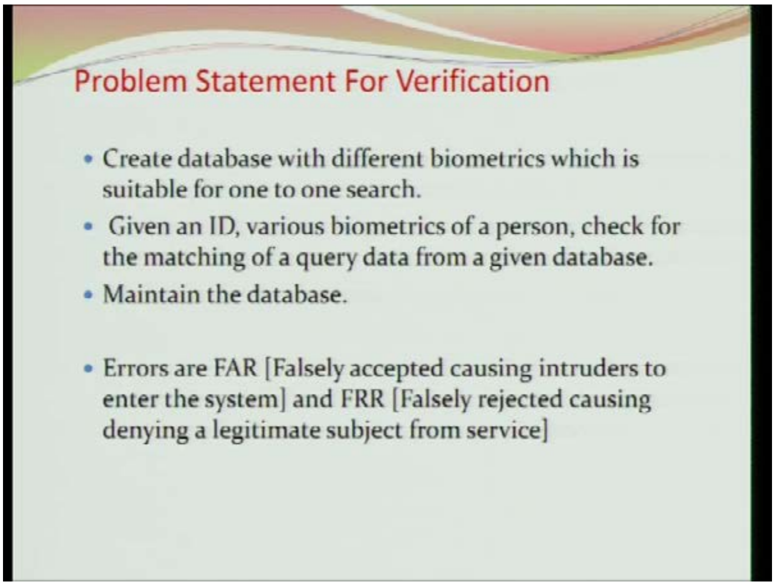
Prof. Phalguni Gupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture No. # 11

Now in the last class, I was discussing about, problem statement for verifications; and there we also discussed, that it is a one to one matching, and different types of errors. And also we told that, the types of database, one is the centralized database, and another one is the distributed database. And where you are using the centralized database, and where should you use the distributed database.

The distributed database will be useful when you are handling or locally some information. Say for example, I want to make the attendance only for this room, and I do not care whether, you are attending the other buildings, class or not. So then it will be sufficient for me that in your card, you come with your smart card, where we put the attendance history or biometrics information.

(Refer Slide Time: 01:22)



Problem Statement For Verification

- Create database with different biometrics which is suitable for one to one search.
- Given an ID, various biometrics of a person, check for the matching of a query data from a given database.
- Maintain the database.
- Errors are FAR [Falsely accepted causing intruders to enter the system] and FRR [Falsely rejected causing denying a legitimate subject from service]

Nowadays, cards are having a huge amount of space. So you can give your biometrics data, and take that information from your smart card, you match it, and you take the decision, and mark on your card itself. So, whenever you surrender your card, you can always find out the history, how many days you are present, which are the days you are absent and so on. Assumption is that, most of the, see I have 41 lectures, or 42 lectures, or 10 lectures, 30 lectures, some number of lectures are there. And the day and I know, my lecture periods, say only Monday, Thursday; Monday, Thursday means 1 and 4. So 1, 4, 1, 4, 1, 4, 1, 4 will be written.

And I the day you are absent, that day it will be marked 0; otherwise, it will be marked 1. So, it is not a very big 41 bits I need, 41 bits I need just to mark whether, you are present or absent. So space wise is not a very big space, and also that you will be storing the feature vectors. Now feature vectors also, I told you that for finger prints say I am keeping the minutiae points, and minutiae points is generally we expect 30 to 40 minutiae points, and each is giving you the coordinates x y, theta, and the type of minutiae points.

So, that means four bytes you need, four bytes into 35, so 140 bytes you need to represent your finger prints says. Now you, with the assumption that, that one I am using once I am using the bytes, the precision is an important thing. So you may not get enough precision, now if I assume that no no sir I want to put real numbers then 140 into four those numbers should be coming, those many bytes will be there. What then you need? You need the machine, must be able to that system, where you would be swiping your swiping your card, must be able to extract the features, and must be able to match. So, that is the additional things, which is not available on your smart card or on your finger print, so that is additional part.

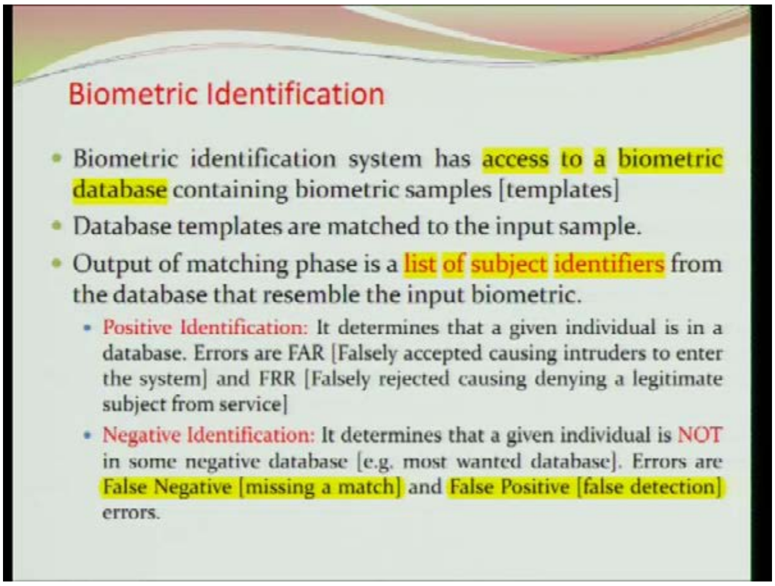
In the case of centralized one, the idea is that, whether I am eligible, to be a member to get a card or if we assume that, you should get only one card, all people are not eligible to enter into this room or enter into the academic area. So, only some valid people are eligible to enter. So I need centralized information, and for that only centralized database is coming in between. Also central database will keep information about the multiple, say for example, finger print is the issue multiple finger prints, suppose one finger due to some reasons is missing or a some problem have occurred so, the finger quality is not coming good. Then you must be able to get the other fingers information on your smart card. So you can tell that, this finger is not giving me the good results. So, system will change your smart card based on your or best quality images. Say sometimes you keep iris say iris data, now I have the left eye and the right eye. So on your card will give you the left eye say, but after time T, I may give you the right eye.

So you have an opportunity, so those information should be kept in your central databases. Say in the case of adhar card, what it has been decided? That in central database you have the enough number of or all sorts of 10 fingers data will be there, your iris will be there, your face, everything is there. But in reality it would be using it would use your only one finger or two fingers based on the need. But while I will be going for another card, and at that time all your data the finger print, iris, all those information would be taken into account to see whether, you have already got any card or not. Because it has been decided that one person should get only one card.

In the case of identification, it is coming with a different problem it is one to N match that means, that if you get some information; biometrics information, you have to find out whether, similar or almost same biometrics feature based, human being exist in the database or not. If exist then you have to return those people, because since you may not get, because you know today you give your biometrics data, and afternoon if you give your biometrics data or tomorrow you give your biometrics data, then you know, you need not be the exactly you will get the same data.

Because you will be looking for the features. Features would be translated, rotated, or noise will be there, all sorts of problem will be there. So you will not get exactly, you should not get exactly same features. Some features may be there, some feature may not be there. So you will be getting a list of people, and this list of people will be useful to identify based on adhar characteristics. So that is the idea, so it will be giving you the end best matches. And suppose nothing is available, no match is available that means you are a new person.

(Refer Slide Time: 08:09)



Biometric Identification

- Biometric identification system has access to a biometric database containing biometric samples [templates]
- Database templates are matched to the input sample.
- Output of matching phase is a list of subject identifiers from the database that resemble the input biometric.
  - Positive Identification: It determines that a given individual is in a database. Errors are FAR [Falsely accepted causing intruders to enter the system] and FRR [Falsely rejected causing denying a legitimate subject from service]
  - Negative Identification: It determines that a given individual is NOT in some negative database [e.g. most wanted database]. Errors are False Negative [missing a match] and False Positive [false detection] errors.

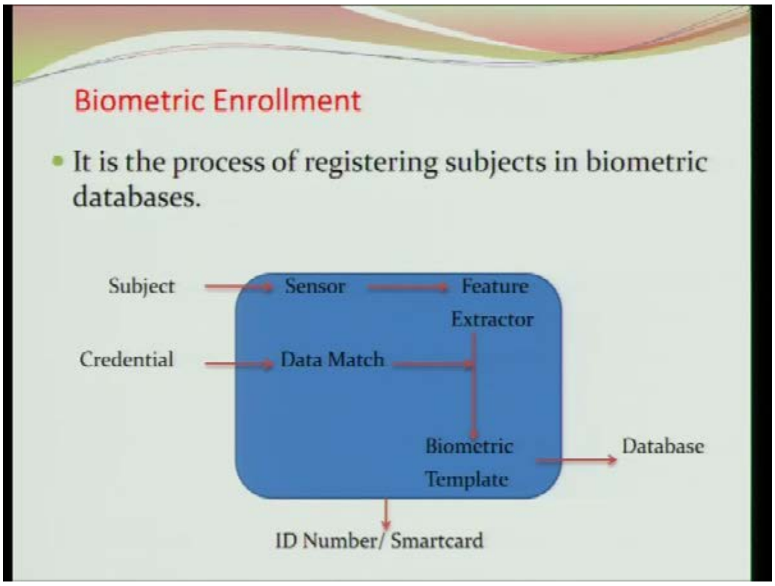
So, your biometric data should be entering into my database, to make it a close environment. So it is expected that, once I am developing a biometric identification system, I should allow using my database whatever; otherwise it will be difficult. So whoever develops the identification system he should be able to access the whole database. And the idea is that your matching algorithm should be able to match the your query template along with all the templates of your database. So, output as I told you, it will give you the list of subjects which are similar or resemble with the input biometrics data.

Now there are two terms I will be using. One is known as positive identification, and another one is positive negative for negative identifications. Positive identification means, it determines all the list of people who are having this list of people available in the database who are having the similar features of query imaging. So obviously there will be two types of error here; one is false acceptance rate, and another one will be false rejection rate. So, to measure the performance of your biometrics identification system for positive identifications, you will be using mainly the two types of error one is FAR, and another one is FRR.

Negative identification means, that it determines it determines that the given individual is not in my database. That means here, database is close with respect to the negative people, not with respect to the genuine people. The other one here, database is closed with respect to everybody. Here, I created a database whom I do not want that to enter in my complex.

And given a biometrics data I will check whether, he is among of those people who are not suppose to enter in my complex. So there will be two types of error. Here, one is known as false negative. False Negative means; that you were suppose to be in that negative list; he was not supposed to allow supposed to be allowed to enter into my complex, but due to some reasons he is through he is through he has been allowed to enter, that is the false negative. And false positive, a genuine person has been considered as he should not be allowed. So this false negative is similar to false accept, and false rejection is similar to false positive.

(Refer Slide Time: 11:23)



Biometric Enrollment

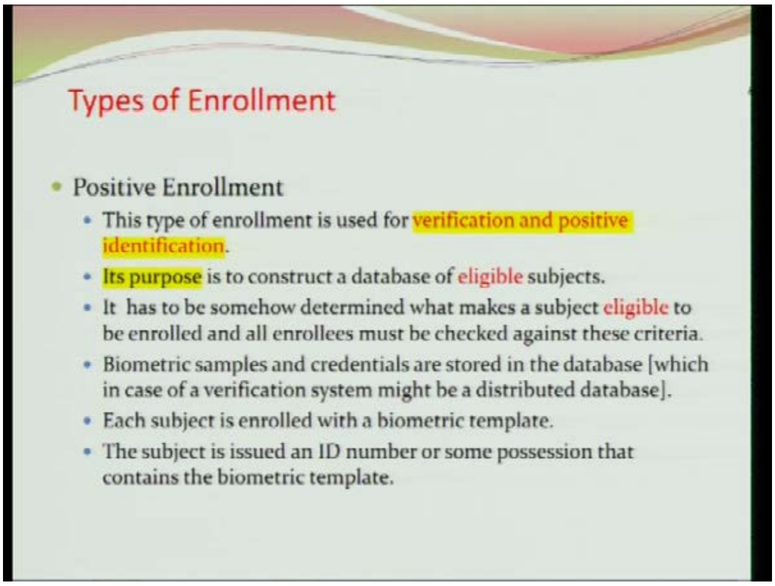
- It is the process of registering subjects in biometric databases.

Now the question is coming that, how to create the database means enrollment stage you have the, what are the things you have. You have a person and or individual, and you have certain credential, certain certificates or maybe I can tell, what is your name? What is your father’s name? What is your date of birth? What is your qualification? all or What is your income? That proves you need.

And something has come in front of the sensor. Sensor gives the accept the data, and once accept the data it extracts the features. And we have also discussed this issue earlier that while accepting the features, he has to do; do several operations, he has to see the weather, quality is image quality of the image is good or not. If the quality is not good you will be asking again and again to give his data. So that, sensor accepts the data with certain quality. And then only feature extractor; extract the features. Credential, the data will be matched because there may be requirement that I want that all those people whose income is less than what 1 lakh rupees per annum. So he need to prove or special category people I want so that he needs to certain information, he has to provide certain information, and you have to check it, yes it is matched, so data has been matched. Using these two it creates a template.

So one thing you remember currently what we are doing is that, I assume the demographic data or the credential data is different from the biometrics data. They are two different entity you come and you based on your credential and also biometric, I could have checked it, but generally once I go I get the card I will give only biometrics data, why shall I show my credential every time. So, but template would be kept made in such a way that it take both the things, and kept ready. Because if required; suppose my biometrics data is not matching I could have told you, show me now since it is not matching, give me some other information tell me your phone number or tell me your something so that it is matching or that can be thought. And based on that you can generate your ID.

(Refer Slide Time: 14:03)



Types of Enrollment

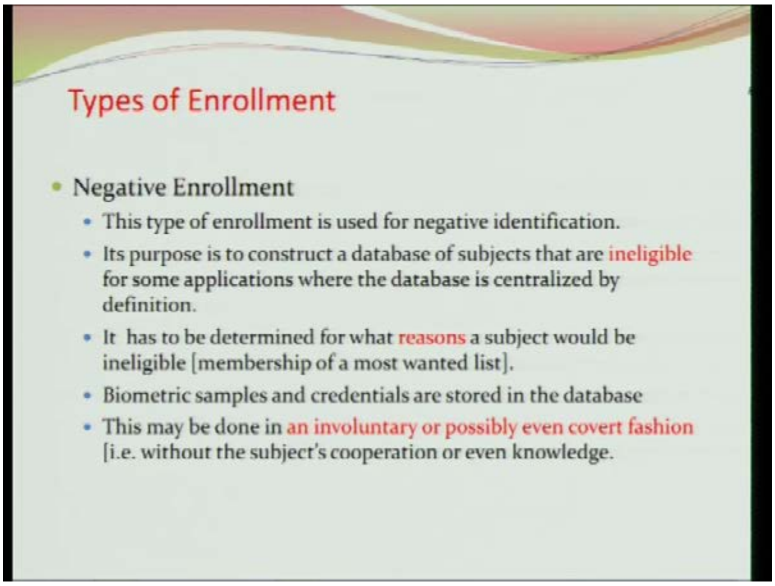
- Positive Enrollment
  - This type of enrollment is used for verification and positive identification.
  - Its purpose is to construct a database of eligible subjects.
  - It has to be somehow determined what makes a subject eligible to be enrolled and all enrollees must be checked against these criteria.
  - Biometric samples and credentials are stored in the database [which in case of a verification system might be a distributed database].
  - Each subject is enrolled with a biometric template.
  - The subject is issued an ID number or some possession that contains the biometric template.

So, the Positive Enrollment, and Negative Enrollment, because you have the two things which is positive database and another one is negative database. So in the Positive

Enrollment what it means that, this will be useful for verification and positive identifications. So here you will be entering all the data who are eligibly in your database. Now the definition of eligible; is my criteria. That criteria is what that, if your income is less than this or if you are below poverty level or if you are some criteria you have you must be all or you must be a citizen of India or some criteria if you prove, if you put, then only you are eligible.

So you will be coming the subject will come with those information's in front of you, somebody will verify. And if it satisfies the requirement, then only you will be allowed to provide your biometrics data. And once you put the data that will be in the form of templates and you will be getting the ID for that purpose.

(Refer Slide Time: 15:08)



Types of Enrollment

- Negative Enrollment
  - This type of enrollment is used for negative identification.
  - Its purpose is to construct a database of subjects that are ineligible for some applications where the database is centralized by definition.
  - It has to be determined for what reasons a subject would be ineligible [membership of a most wanted list].
  - Biometric samples and credentials are stored in the database
  - This may be done in an involuntary or possibly even covert fashion [i.e. without the subject's cooperation or even knowledge.

In the case of negative, it is completely different. Negative Enrollment, here first thing is that; it is used for negative identifications. And in the database whom you are keeping, those who are not eligible those who are not eligible to enter into my complex, their data will be there. Now how can you tell that I am not eligible? Because you know it is a very sensitive one, if I tell you that do not enter into my complex, you are not eligible you will feel bad. Everybody will feel bad everybody has certain sense of sense of whether I should be honored or not. Suppose you tell, no no you are not eligible to my complex, it will be you have to justify why you are not allowing him. So that is you have to find out what credential? Negative credential he has, so that you are not allowing him.

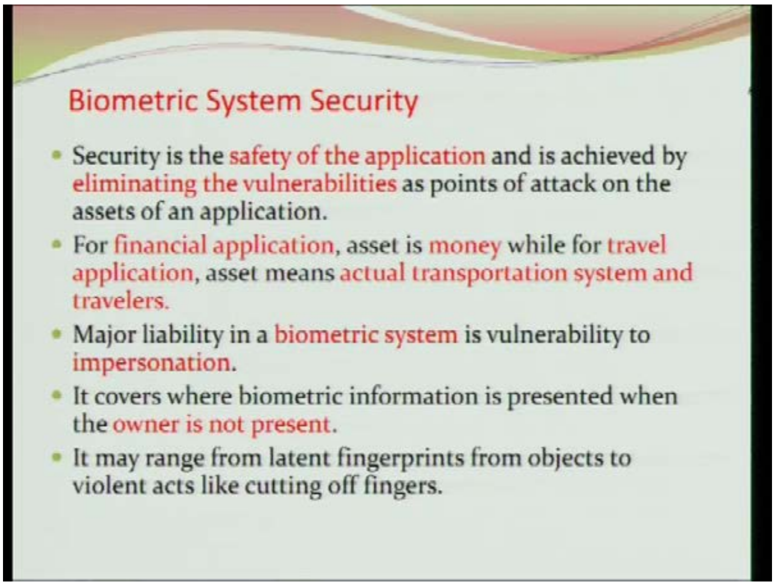
Suppose in my complex I do not want to allow those who take, say kuttka. Nowadays that tradition is going on kuttka will not be allowed, so kuttka people I will not allow. Also I am telling that ok those who are having the habit of stealing something, these people are also there will be you know different types of people. So but, a person who takes kuttka, he may not be a thief. So you have to write down specifically that, these person I will not allow who because he takes kuttka, this person I will allow I will not allow because he is a thief, and this persons I will not allow because he is both of the, they are taking both of the, he is satisfying by both criteria, all those credential must be written carefully.

Now once you come, there is a possibility that you are taking kuttka, but your system database does not contain your name, because you have fixed this people name over there. You will be allowed to enter into the system. So that is a basically those issues should be clear, because you can tell that yes you are allowing him but, you are not allowing me satisfying both the criteria right. He is also taking kuttka, I am also taking kuttka, but you are allowing him, but you are not allowing me; this is not a correct thing.

So those things should be pinpointed, so that you do not face problem. Now one thing is that this data will be involuntary. Nobody will come forward to tell you that I take kuttka, so do not allow me to enter. It is the authorities, who are to decide; who are not allowed, and who will be allowed, and so it you have to take this information under, convert Covert operation; it is a covert fashion. Covert fashion means that do not you should, but he should not know he should not know because otherwise it may dishearten, it may create problems and so on.

So you may not get because cooperation from the concerned person because even if you ask that ok I have not allowing you but, you have to give your biometrics data. Then you he will not come forward right, he does not want that my name should be or his name should be in the list. So what what you are thinking, that I cannot think where his finger print is required. He will not give you the finger print, because once if he comes to know that, if I give my finger, his finger print; then he will be barred from entering into the residence. So face may be one possible solution, where you take hidden his photograph and enter into the system. This I have covered.

(Refer Slide Time: 19:20)



Biometric System Security

- Security is the safety of the application and is achieved by eliminating the vulnerabilities as points of attack on the assets of an application.
- For financial application, asset is money while for travel application, asset means actual transportation system and travelers.
- Major liability in a biometric system is vulnerability to impersonation.
- It covers where biometric information is presented when the owner is not present.
- It may range from latent fingerprints from objects to violent acts like cutting off fingers.

Now the biometrics system security, what does it mean security? You know what does what does it mean that my room is secure? Can you tell me the room is secure?

(( ))

Enough, necessary intervention must not be there. Suppose one way that you can lock the room, so room is secured. Does it secured? It is secure with respect to thief, but it is not secure with respect to fire. So you have to define carefully what is security? Now the thing is that security is the safety of the application, whatever application you want to make it safe. So what is that it can be achieved by who by eliminating the vulnerabilities as point of attacks, on assets of the application; so you have certain assets of the applications, and every asset has certain vulnerabilities. For this room you may be that projector has some vulnerabilities, so you have to think that there exists certain point of attack, those should be eliminated. That is an important thing.

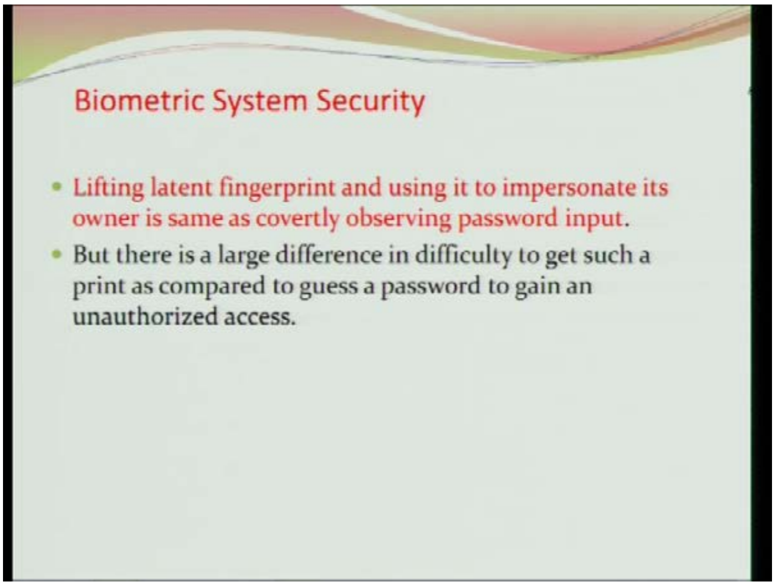
So in the financial application the asset is money of course, that is I should save my money, that is the in case of financial application. In my travel application, you must ensure; that traveler is safe or the transportation you are using that is safe. So this asset what is variable, it depends upon the environment where you are using. So secure my asset is safe; what is the type of asset, based on that you will be deciding what type of security is required.

Now in the case of biometrics system, the vulnerability is the impersonation, because biometrics is also system, is also an asset. So is vulnerability with respect to the impersonation. Now, what does it mean that impersonation? you know it goes worst, when you know somebody wants to make use of your biometrics system or wants to use your system, even without your presence, that is the up to that level you one can think. One is that I can force you give me your biometrics information, sign on this paper forcibly, and then I withdraw the money or whatever I do, this is possible. Another one is that I am not there, and you have withdrawn my money.

So that is a level, so it can range from the latent fingerprint from the objects. Say what happens, on your, suppose you take a glass of water right, and after taking the water your fingerprint will be there, that is known as latent finger print. And from there also I can determine your fingerprints, then I can have a mask on it, and then I can prepare a plastic cover or using your mask, and I can put on my finger, and I can make use of it. So the latent fingerprint from objects, to the violent acts; like cutting the fingers, and so on. So by cutting the finger I will tell that my finger print is not, my finger is not correct or it is not it is the affected one so I cannot provide you with the data. So I will give other information and give my money; so all those issues are there.

Now thing about this latent fingerprints, does it not similar to your password stolen; say for example, in the latent fingerprints what happens? That I will lift your fingerprints from the objects, where you have given your finger prints, then what I will do? I will take the photograph of that fingerprints, and then process it; then I will prepare one mask on it, and I will put those information on that mask, and then I will cover it, and I will withdraw your money provided that the sensor does not have the concept of dead finger or live finger.

(Refer Slide Time: 24:33)



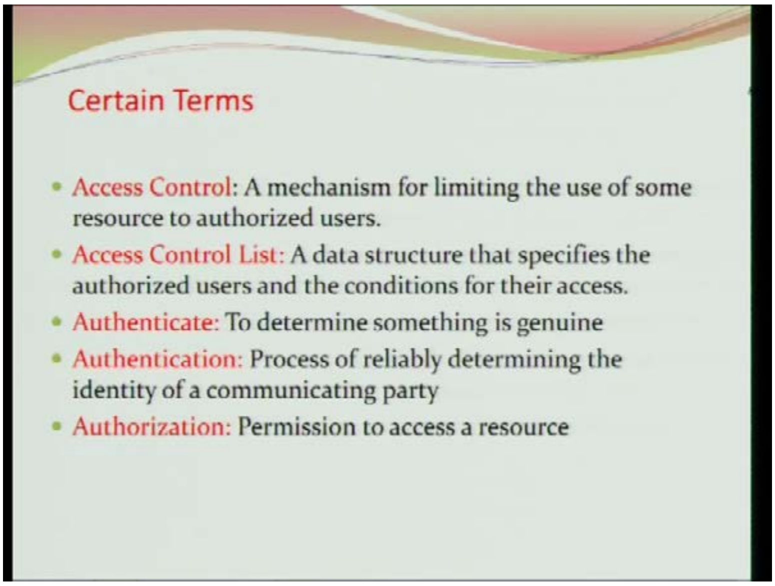
Biometric System Security

- Lifting latent fingerprint and using it to impersonate its owner is same as covertly observing password input.
- But there is a large difference in difficulty to get such a print as compared to guess a password to gain an unauthorized access.

So, what happens that you have given unknowingly your fingerprints on some objects, and that has been used. Similarly, that password is also the same thing; knowingly or unknowingly somebody has come to know your password, and he can make use of it. So the problem is same, only thing is that degree of difficulty is different. The knowing password is a four digit number, and I know that your behavior, your different knowledge, based on that I can determine; what is your password, but this is not the case with the fingerprints, he has to put lot of efforts.

So degree of difficulty different, and I will be using only this one, if the value cost I need to spend to determine my fingerprint cap must be much much less than the money I will be getting through this process, otherwise what for I will be I have been doing all these, and I will steal the biometrics data because that will not be use I have spent huge amount of money, I have spent huge amount of time but, in return if I do not get anything, does not make sense.

(Refer Slide Time: 25:51)



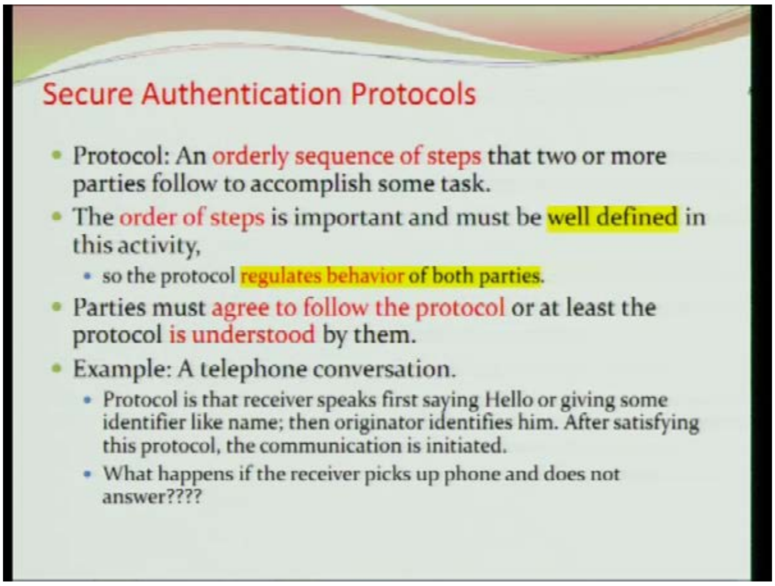
Certain Terms

- Access Control: A mechanism for limiting the use of some resource to authorized users.
- Access Control List: A data structure that specifies the authorized users and the conditions for their access.
- Authenticate: To determine something is genuine
- Authentication: Process of reliably determining the identity of a communicating party
- Authorization: Permission to access a resource

These are the very easy and different terms very frequently you will be using while we would be discussing about the biometrics system.

Say, I want to put biometrics data on my server room or biometrics entrance in server room, so the term you will find in one is the Access Control. It is a process to limit the people to enter into a system or so this is the thing, a mechanism for limiting the use of some resources to the authorized user. Access control list, is the list of people who can use the your system. Authenticate this is just English word to determine something which is genuine. Authentication is the process by which you will be telling that yes, he is a genuine one and his identification has been verified, and he may be allowed to use a system, and authorization is nothing but, the permission to use the system.

(Refer Slide Time: 27:02)



Secure Authentication Protocols

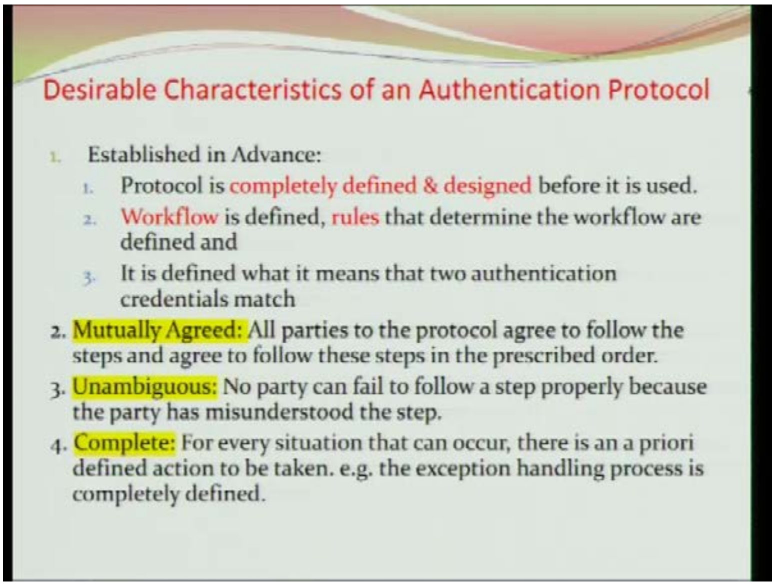
- Protocol: An orderly sequence of steps that two or more parties follow to accomplish some task.
- The order of steps is important and must be well defined in this activity,
  - so the protocol regulates behavior of both parties.
- Parties must agree to follow the protocol or at least the protocol is understood by them.
- Example: A telephone conversation.
  - Protocol is that receiver speaks first saying Hello or giving some identifier like name; then originator identifies him. After satisfying this protocol, the communication is initiated.
  - What happens if the receiver picks up phone and does not answer????

This is the commonly used things secure authentication protocol. A protocol is what, an orderly sequence of steps this is the one thing, it is not the sequence of steps, it is a orderly sequence of steps that two or more parties follow to accomplish the task, suppose you have a task that has to be solved or that has to be done by two or more parties, then you have to have certain orderly defined steps orderly sequence steps, the order steps is very important, it must be well defined. Otherwise protocol fails to regulate the behavior of the parties. So party must be; all the parties must agree to follow the protocols; that is the first criteria. At any stage they should not tell I have not understood the protocols any protocol, so this is the important properties on protocols.

Say for example, the telephonic conversation this is a very common thing. Suppose I give a call on your mobile, what do you do? You tell hello, suppose you do not tell hello, hello is the, if you tell hello then I tell hello or I am phalguni speaking something I will tell or you will be telling your name, instead of telling hello, some something is there. Once you tell hello or you tell your name or something, and I listen that one then I will tell my name, then you will accept my name then match occurs, then only that you would realize that, two genuine parties wants to talk to each other.

But if I call you and you do not speak, you are just sitting idle then what I will do? I will feel that most probably that this link has not been established, there is some problem he is not getting my call, so I will detach. Again I will tell, till you tell hello that is the general way. Now another thing is that once I ring, and I call you what are you telling; you start telling all abusive language is there a possibility. You will not do because you know what is this, so that is it does not allow the in your protocol.

(Refer Slide Time: 29:46)



Desirable Characteristics of an Authentication Protocol

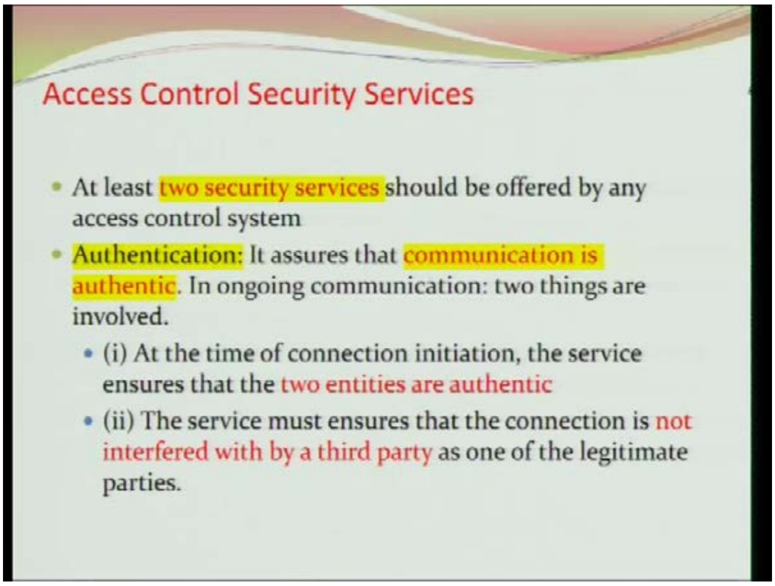
1. Established in Advance:
   1. Protocol is completely defined & designed before it is used.
   2. Workflow is defined, rules that determine the workflow are defined and
   3. It is defined what it means that two authentication credentials match
2. Mutually Agreed: All parties to the protocol agree to follow the steps and agree to follow these steps in the prescribed order.
3. Unambiguous: No party can fail to follow a step properly because the party has misunderstood the step.
4. Complete: For every situation that can occur, there is an a priori defined action to be taken. e.g. the exception handling process is completely defined.

So what happens, that this protocol is completely defined and designed before it is used. It is a well defined, and it is not that on the spot you define that this is should be our protocol this is well defined. Say sometimes you use code language also, but that code has to be well defined; otherwise the other part will not establish the link it will not be possible, so this well defined. And then you should have the proper workflow. Now in the Workflow there will be certain steps to be followed. In each step, there are certain rules, certain rules that should be well defined; there should not be any ambiguity in any stage so that you are sitting idle.

Say for example, if I call you, and you are just sitting idle; then there is an ambiguity that you do not know what to do if I receive a call, then what shall I do with this, but that should not be there, it should be well defined one. And then there should be certain ways, certain technique by which you will tell yes this is two credential are matched so you can, they can talk to each other. So this is the established fact; the protocol established fact. Now this coming the Mutually Agreed, that whatever workflow, whatever rules you define all the parties must agree that yes, we will follow this, you cannot tell at any stage that do not know, I do not agree, I did not agree to this, whatever you decided; you decide, you should decide at priority and everybody has to follow accordingly Unambiguous, that nobody should tell that I fail to do this thing, because I did not understand the rules, I did not understand the protocols or I did not understand the workflow. So that is why I did not follow that one. So that is unambiguous. Then complete, complete means that, at any stage what happens? there is a possibility you do not know what to do under this? What rule I will follow? So that is that should not be there even does not exist any rules, there should be an exceptional handling situation which also will be well defined that under this circumstances, these steps to be followed. If you do not have any answer on this, you cannot just cancel the things, because I did not understand.

So, there are people they do it while telephonic conversation. This is an example telephonic conversation; what happens that you are in a big problem you just cut that you do not want to go further, so you stop it. So, but that is not a good practice there are several people you know at the end, he forgets to tell either bye or something let me stop my discussion or let me keep it; something like that. The protocol feels, that you should tell that; yes let us stop now discussion, we will talk to you later. But several people; they do not speak; they just switch off or cancel the link.

(Refer Slide Time: 33:30)



Access Control Security Services

- At least two security services should be offered by any access control system
- Authentication: It assures that communication is authentic. In ongoing communication: two things are involved.
  - (i) At the time of connection initiation, the service ensures that the two entities are authentic
  - (ii) The service must ensures that the connection is not interfered with by a third party as one of the legitimate parties.

Now in any system, it is expected that; there are two at least two security services, in access control also it is expected that there will be two at least two security services. One of them is authentication right, and the other one is non reputation. Now what is authentication here, that in the case of communication it is authenticate, the communication is authenticate.

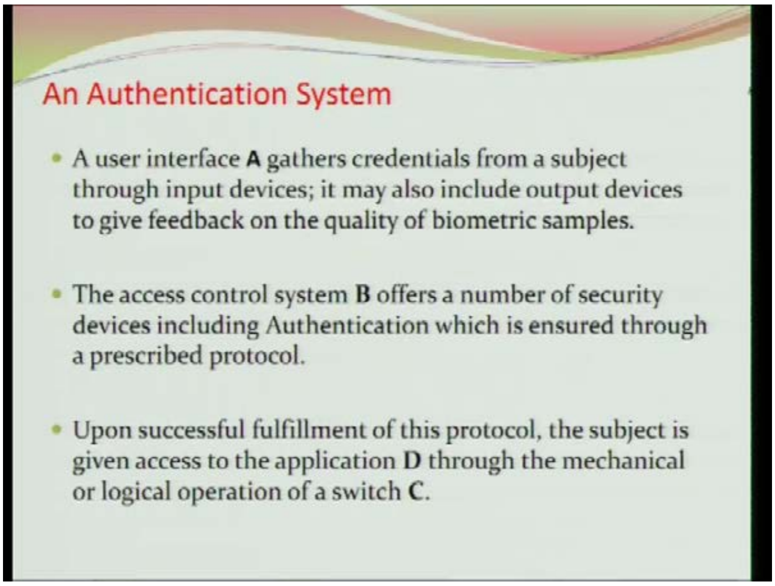
What it means? suppose in the case of communication I want to talk to another person so if I dial it the other person also will give the through protocol it will be link will be established, yes I will listen him, and I will understand that he is the genuine man; whom I am asking, who I am looking for. Suppose you make a call, and you get a voice from somebody you must understand, yes he is the man whom I am talking; otherwise suppose I call and I am realizing the I have received a response, but it does not look like that his voice it is there is a possibility sometimes it happens. Somebody else picks up the phone, so you will not start telling all the history that this is the thing you have to ask him, that you have to understand that who is the person there, is it the same person whom you are looking for. If only then there is a match occur, otherwise you will be looking for that man that is the standard practice.

So first part is that this once you this initiation, a connection is initiated that you must ensure that it both the parties are genuine. Second rule is that there should not exist there should not be another third party who is tapping your thing, who is also listening your, who is also not connected in your system, so that is the thing that you must ensure that there exist, there does not exit a third party who is interfering your activity.

Now the second service what we are thinking non reputation, what it means that, it prevents both the parties for denying the transmitted message when that, if a message is sent, then receiver must have the prove that, yes he has sent me this message, and the same time, if a message is received by somebody then sender must have the prove that he has send this and it has been received by him.

So this is the most important service what we expect from any security system. It says that the confidentiality is another important thing, which anyway, because if once I tell that it is secured then it should be confidential.

(Refer Slide Time: 36:43)



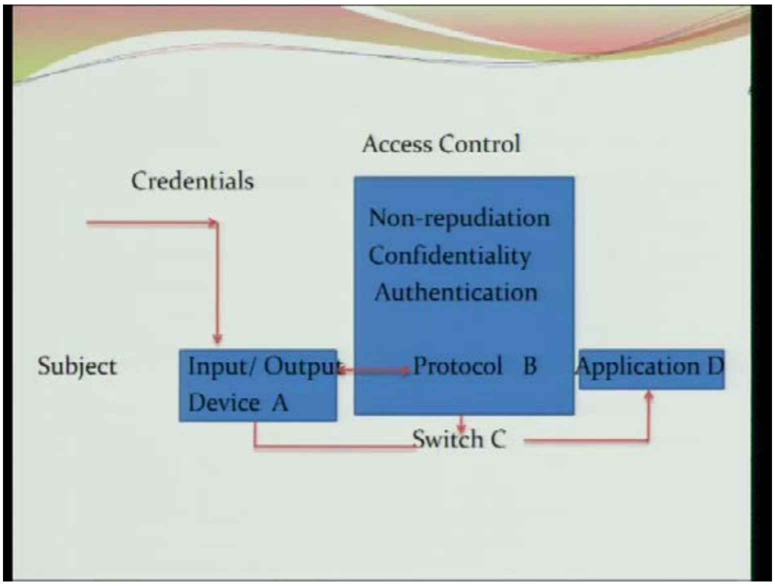
An Authentication System

- A user interface **A** gathers credentials from a subject through input devices; it may also include output devices to give feedback on the quality of biometric samples.
- The access control system **B** offers a number of security devices including Authentication which is ensured through a prescribed protocol.
- Upon successful fulfillment of this protocol, the subject is given access to the application **D** through the mechanical or logical operation of a switch **C**.

Now, consider an Authentication System, so there will be one device to collect the data credential, so let us assume that you have a credential A which gathers all your credentials, and then it verifies that these credentials are correct. If required you will be having an output device to show you that, yes this is the credential you have given, this is the quality of your credential, and so on. Once you accept that, yes I agree with all of, and then only the system A will transfer the data to the next system, which is authentication system.

And in the authentication system what it does? He checks all your credentials, he accepts, he determines the features, and these features will be matched with your data base, and if it is matched then he sends to the system C who will be telling yes you are the genuine person so you will be allowed to use the other whatever service you want to perform.

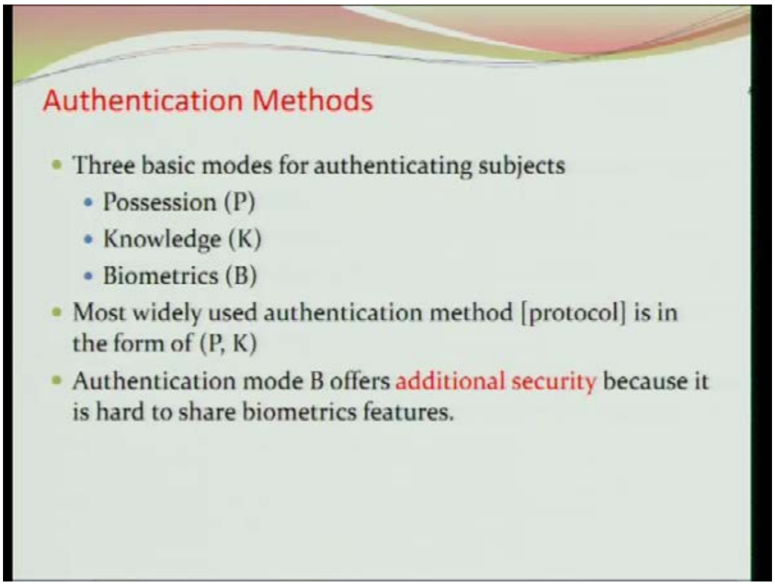
(Refer Slide Time: 38:06)



So the one example is, the your; again once you have given one there to adhar card to give your data, they have done all typing, they have taken your all demographic information’s, then they have showed you. Do you agree with all of that, that if you tell no I do not agree, then they will try to correct it, again if you tell that no this is not this should be this and then they will do it and after showing that then they will tell ok, now agreed then you have to press a key or you have to take a; give a signature then only you will be allowed to go to another device for giving your biometrics information. Once it is here then the template would be created.

And, the next that access control things will have, say for example, when I am telling the demographic data, say I am from east, and I have come to North India to give you my biometrics data; I face big problem, say my name is Phalguni Gupta. Now they will always write in Hindi ‘ah’ Gupta, ‘ah’ is there in Bengali it is Guptu, so I also do not know, how to write in Hindi what is Gupto ‘o’ will be there or will not be there because in Bengali there is no ‘o’ concept, if it is there it is always there otherwise, it is not there something like that. Same thing, if I go from north India to south India this problem will be there all sorts of them, and you know; and they will write in Hindi and you have to read in Hindi I may not know Hindi, and all those issues are coming in between. Anyway that this device, play that role.

(Refer Slide Time: 40:07)

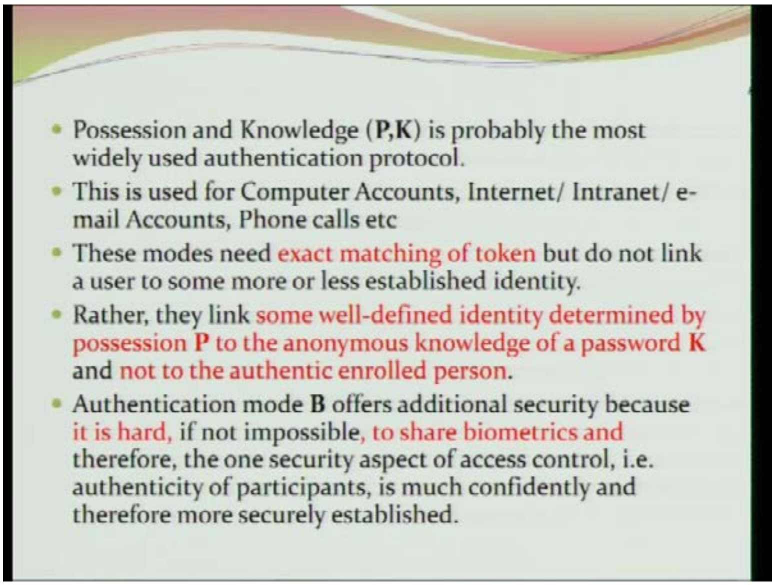


Authentication Methods

- Three basic modes for authenticating subjects
  - Possession (P)
  - Knowledge (K)
  - Biometrics (B)
- Most widely used authentication method [protocol] is in the form of (P, K)
- Authentication mode B offers additional security because it is hard to share biometrics features.

By now all this terminology you have understood, but completeness sake I am covering again that, one is the possessions is P, another one is knowledge, another one is biometrics. So, P K B will be used very frequently. But most widely used is P and K that not only possession, but also your knowledge. And biometrics gives you additional security because it is hard to share.

(Refer Slide Time: 40:46)



- Possession and Knowledge (**P**,**K**) is probably the most widely used authentication protocol.
- This is used for Computer Accounts, Internet/ Intranet/ e-mail Accounts, Phone calls etc
- These modes need exact matching of token but do not link a user to some more or less established identity.
- Rather, they link some well-defined identity determined by possession **P** to the anonymous knowledge of a password **K** and not to the authentic enrolled person.
- Authentication mode **B** offers additional security because it is hard, if not impossible, to share biometrics and therefore, the one security aspect of access control, i.e. authenticity of participants, is much confidently and therefore more securely established.

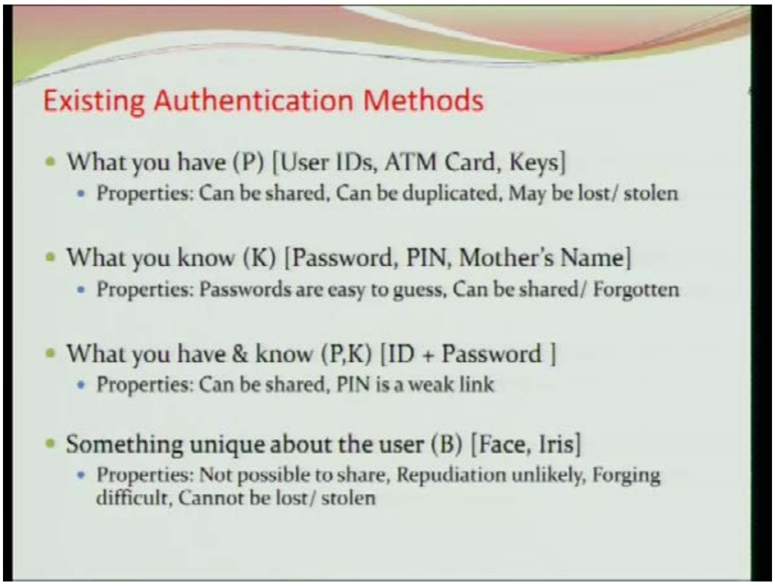
So this (P,K) is used mostly because in computer accounts, internet, intranet, e-mail accounts, phone calls etcetera. Now they hear that, one issue is that, once you are using

(P,K) method, then first part there whatever you use that should be exactly matched. That if you use the password or knowledge, that knowledge has to be matched exactly whatever you have stored there. If you use the car key, to open the door then that key has to be matched exactly with the same (( )) part inside right, otherwise you cannot establish the link. Now the issue is that, you have the knowledge, and you have the under possession something, based on that you are identifying that I am the man which is not correct.

See, by showing the whatever, you under your possession by showing a whatever, knowledge you have, you can prove that I card contains all the information. Suppose, but you cannot prove that I am the person because I have this information's so that is the major problem here, but it is not the case with biometrics. But the problem with the biometrics is something different. Here in the case of possession, and knowledge that, I if I misplace my card, and I lost, I forget my knowledge then you are in problem, if somebody knows that whatever you your password, and somebody knows whatever is the key he can also use your thing. But in the case of biometrics that is not possible, because you are not sure of it.

But issue is that, that biometrics data will not give you exact match later on. In the case of knowledge or possession, that must be exactly matched; one to one match then only, but in the case of biometrics even though it is not sharable but, you will not get exact match.

(Refer Slide Time: 43:09)

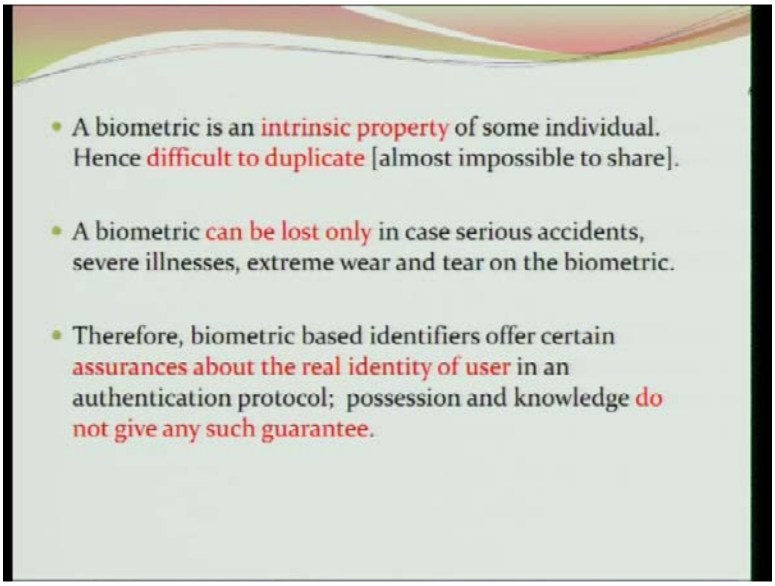


Existing Authentication Methods

- What you have (P) [User IDs, ATM Card, Keys]
  - Properties: Can be shared, Can be duplicated, May be lost/ stolen
- What you know (K) [Password, PIN, Mother's Name]
  - Properties: Passwords are easy to guess, Can be shared/ Forgotten
- What you have & know (P,K) [ID + Password]
  - Properties: Can be shared, PIN is a weak link
- Something unique about the user (B) [Face, Iris]
  - Properties: Not possible to share, Repudiation unlikely, Forging difficult, Cannot be lost/ stolen

So, in a case of possession property; that can be shared, can be duplicated, and may be lost or stolen. In the case of knowledge it is easy to guess, and can be shared or forgotten, and in the case of both knowledge and possession can be shared. In the case of biometrics it is not possible to share, repudiation is unlikely, Forging difficult, and cannot be lost or stolen. This is mostly I have covered.

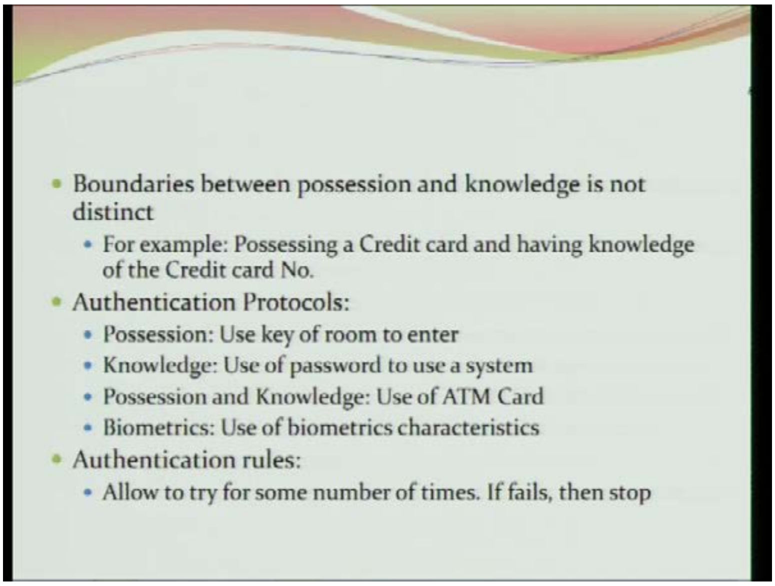
(Refer Slide Time: 43:44)



- A biometric is an intrinsic property of some individual. Hence difficult to duplicate [almost impossible to share].
- A biometric can be lost only in case serious accidents, severe illnesses, extreme wear and tear on the biometric.
- Therefore, biometric based identifiers offer certain assurances about the real identity of user in an authentication protocol; possession and knowledge do not give any such guarantee.

Except that, biometrics can be lost only when there is a serious accident or severe illness or due to some other reasons.

(Refer Slide Time: 43:58)



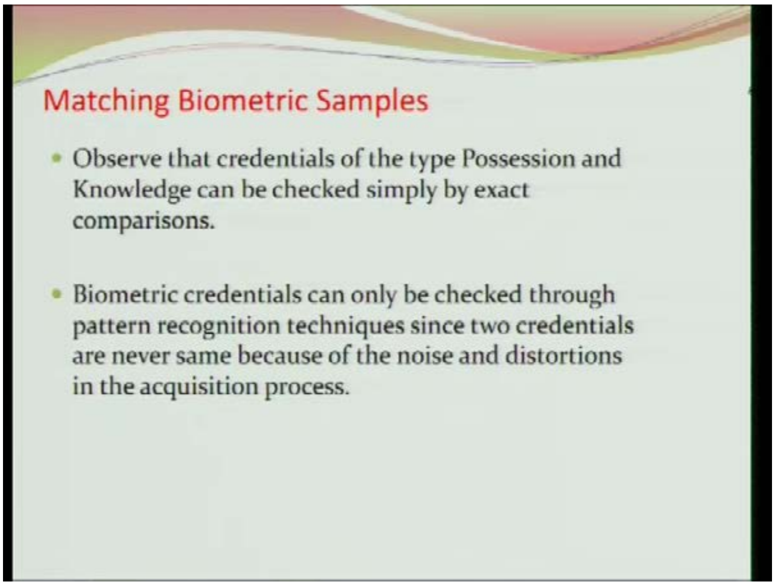
- Boundaries between possession and knowledge is not distinct
  - For example: Possessing a Credit card and having knowledge of the Credit card No.
- Authentication Protocols:
  - Possession: Use key of room to enter
  - Knowledge: Use of password to use a system
  - Possession and Knowledge: Use of ATM Card
  - Biometrics: Use of biometrics characteristics
- Authentication rules:
  - Allow to try for some number of times. If fails, then stop

Now, if there in a boundary between the possessions and the knowledge; there is a big problem that, which part you can tell this is under possession, which part you can tell this is under knowledge. For example that a credit card. Now in the credit I need the or in the ATM card I may place I may need also ATM card and also ATM card number. So card number you have to remember, it is in their knowledge or pin is your knowledge, and card you have to swap the card so the card is also has to be there. So there is a no there is a difficult to tell that this is a part up to you tell that it is a possession, this is your knowledge domain. So this has to be difficult, but in the case of in the case of biometrics, it is not that it is completely separate entity.

The possessions, use the key of a room to enter. Knowledge, use the password and Possession Knowledge, is the use the ATM card because it contains both the information’s. And Biometrics is the biometrics characteristic. Now authentication rule is that you will be allowed several times say 5 times, 6 times after that automatically it will stop we will not allow you to go here. Have you used the ATM card with different pin, Have you tried? Without using exact your pin somebody else pin you use and you use your card, did you try? After five attempts it blocks the card. And then what you do? You go to the bank; then bank will tell come after three days, then what happened by three days I cannot withdraw my money. See now a days it is blocking the card earlier days initially when it started, so after 5 attempts the card vanish, card goes inside.

You have to go inside to the manager, to get the card back. So here, if it fails then we expect the stop. But if you see the Gmail account or yahoo account; and you give some wrong password or you have forgotten anyone to type whatever, it gives capture that, and the capture is such a complicated one, it is not a readable. Sometimes they put the down capture. Down capture means two captures, and one on the top of another one, so which one is coming, and they are not valid word also sometimes, if it is a valid word you can guess, but that is not valid word some random characters are there.

(Refer Slide Time: 47:02)

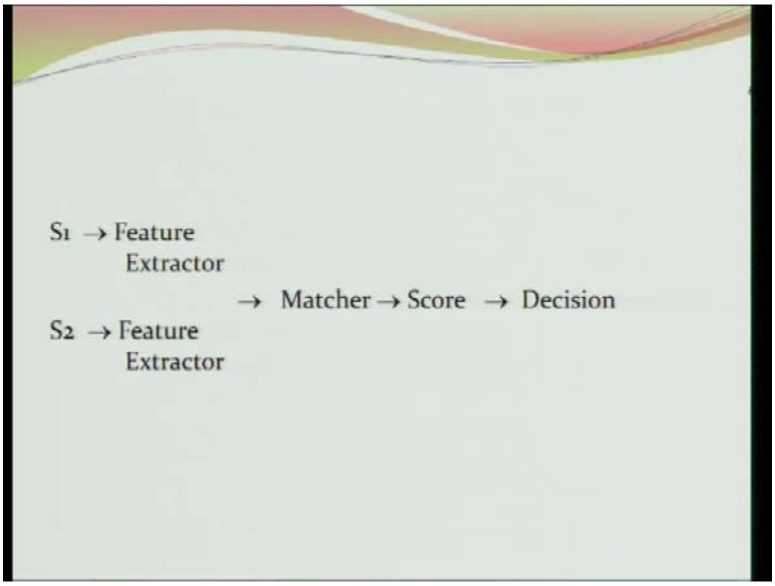


Matching Biometric Samples

- Observe that credentials of the type Possession and Knowledge can be checked simply by exact comparisons.
- Biometric credentials can only be checked through pattern recognition techniques since two credentials are never same because of the noise and distortions in the acquisition process.

So matching the two samples in the case of pin, it is exactly matching, but in the case of biometrics it is not the case, it is pattern matching. So pattern matching will never give you the exact solution, as I have telling you there will be lot of noises, so you have to use the word threshold. How much or What is the percentage that it matched with the patterns, so that threshold is very important parameters fort biometric system, and that threshold is dependent on the sensor, it depend it should depend on the atmosphere, it should be dependent on the control environment, non control environment, all those factors will be coming into the picture.

(Refer Slide Time: 47:50)



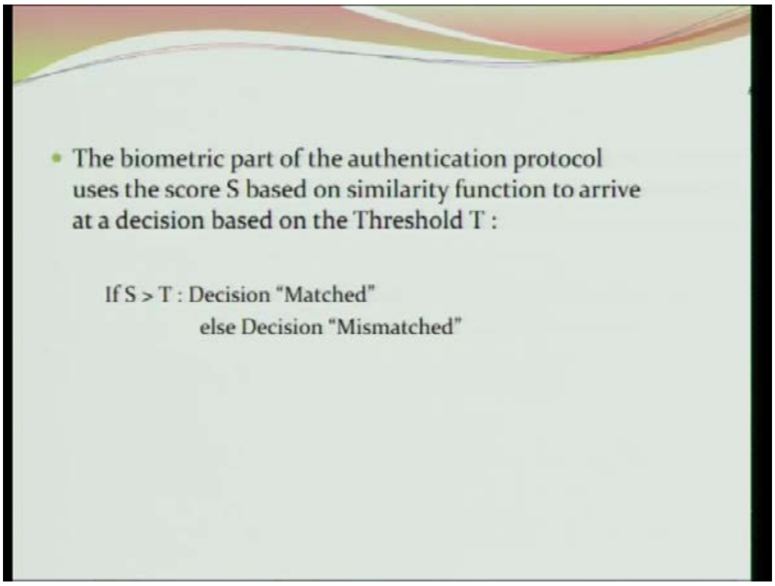
S1 → Feature Extractor

→ Matcher → Score → Decision

S2 → Feature Extractor

So the structure is that have the feature extractor. Subject has comes feature extractor, feature extractor, matcher, score, and decision; that decision is the important thing now. Because your matcher is what matcher is nothing but now you will be finding some distance formula, through which you will be telling how much percentage? Or what is the percentage is matched? And that will give you the score. Now the based on the score you have to take that decision.

(Refer Slide Time: 48:19)



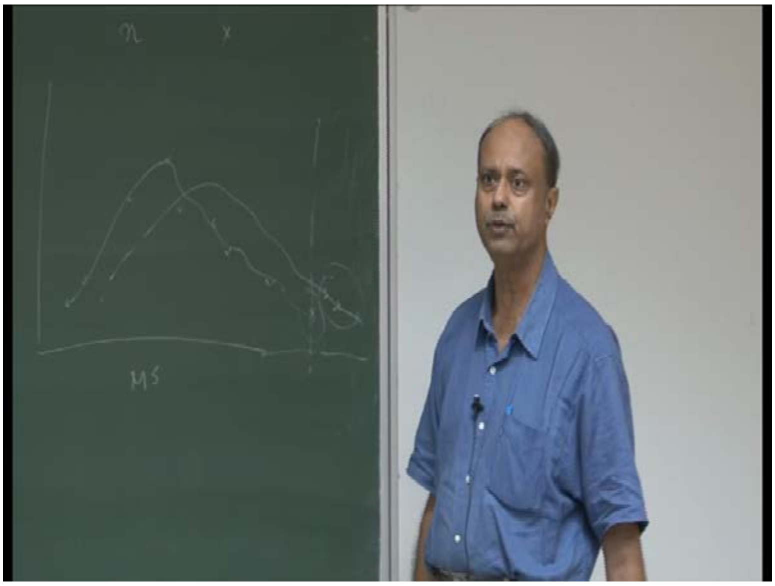
- The biometric part of the authentication protocol uses the score S based on similarity function to arrive at a decision based on the Threshold T :

If S > T : Decision "Matched"
else Decision "Mismatched"

So, if the score is greater than threshold then it will match, otherwise it does not match. Now greater than the score means what; greater than the score means that, this is similarity match, if these two are similar then hundred percent should be match, if it is completely too different then it should be zero percent match.

In the case of dissimilarity the symbol will be different, if S is less than T, then decision is matched; otherwise decision is not matched. Now you take the two fingerprints and both of them are having say above 30 minutiae points probability that at some of the fingerprints some of the minutiae points are matched is very high. You will get at least get 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, some numbers there minutiae points will be match. You will not you will not find a case, where that these 2 minutiae point of these two finger prints are such that, does not exist any fingerprint, minutiae point which are not matched, it is not that. So matching score will not be 0.

(Refer Slide Time: 49:51)



Now once you get matching score. So, what you get? I will have matching score, and you have a set of people, say population size is n, and one query image has come, and that query image will be matched with him, and you will get one matching score. So the matching score is this, another matching score will be like this, some matching score will be getting, some of them will be like this, some of them here.

So you can have some this type of graph so this has been matched with n people then matching scores some people will have almost same, some will be very less, people will have exact match and so on. So this is known as matching score versus frequency graph. Now, suppose I assume because you want to match suppose this is the genuine person that x is there and this is the person, so you will be putting your threshold is like this.

So that you are accepting only this man, remaining will be thrown out. Now this threshold value cannot be different for different persons see another person is there his graph is also like this and his threshold value is here the genuine man so if you consider this is my threshold value then this man will be out. Agreed? Now suppose you consider this is the threshold value that this is him this man is also in then but, there may be some other person here some other people.

Then all of them all of them also would be in so you are falsely accepting this people so this selection of this threshold; First part I am telling that, it cannot be dynamic, it cannot be, you cannot decide for this man session value is this, for that man threshold value is this, that you cannot do. It is not feasible. Second part is that your threshold value cannot be, will not be such that only genuine people would be accepted, it is not possible. So by that process you will be accepting some people and if you do not accept. Suppose I consider this then you would be rejecting this man, genuine person which is falsely rejected.

(Refer Slide Time: 53:00)

So if you see, that if you consider that different threshold and versus the matching score. Now you will be getting the different thresholds and in another side there will be matching scores, so you can obtain the matching score verses threshold graph. And based on that, you can obtain the different types of what is the optimum value of your threshold. So that you can, you know satisfy your requirement. Now to satisfy your requirement is the difficult or is that depends on the application. For example, I want that any transaction in bank means that it is more than 5 core rupees. So, if it is more than 5 core rupees is a very big number. So I will not allow any false accepted people.

I do not mind to reject the genuine person, because the money is very costly. So here constant is that my threshold would be such that falsely accept would be 0, and whatever false rejection comes I do not mind. The other case is that class attendance, where I do not mind if somebody wants to come and attend extra percentage then no problem, I know that people will not come to extra class, even if you are so selfish you attend only his class, because he gives a good grade in his class.

So in that case false acceptance is not a problem, but false rejection is the issue. So your threshold should see that constraint that what should be the approach so people will ask you that, what the false acceptance, so once you tell your false acceptance rate is 0 corresponding false rejection rate will come out based on your threshold value. So there are three parameters one is that false rejection rate, another one false acceptance rate, another one threshold value, if one you define; other two automatically you can define from the graph.