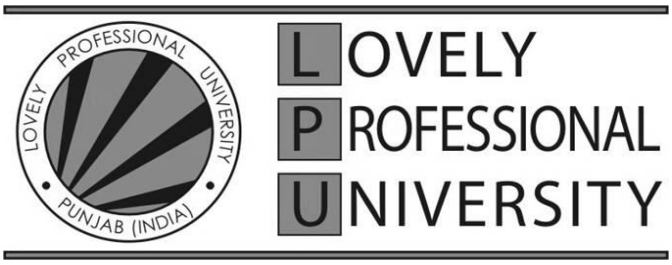

Implementing Kerberos for Web Service Security

A Dissertation submitted

By

Sunny Gupta

to

Department of Computer Sciences

In partial fulfillment of the requirement for the

Award of the degree of

Master of Technology in Computer Sciences (Part Time)

Under the guidance of

Mr. Gurpreet Singh

Assistant Professor, CSE

(June 2014)

CERTIFICATE

This is to certify that **Sunny Gupta** has completed M.Tech Dissertation titled '**Implementing Kerberos for Web Service Security**' under my guidance and supervision. To the best of my knowledge, the present work is the result of her own investigation and study. No part of the dissertation has never been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.Tech Computer Science & Engg.

Date:

Signature of Advisor

Name: Mr. Gurpreet Singh

UID: 16523

DECLARATION

I hereby declare that the dissertation proposal entitled, Implementing Kerberos for web service security submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: _____

Investigator

Regd. No.41100060

ACKNOWLEDGEMENT

I am grateful to **Mr. Gurpreet Singh, Assistant Professor, Department of CSE,** for their immense knowledge, competence and dedicated support; besides their busy teaching schedule and other responsibilities.

I appreciate the motivational words for my friends for their extending help directly or indirectly.

Lastly, I sincerely pay homage to Almighty God, Parents and other members of my family for their blessings, boundless love, sacrifice encouragement constant inspiration emotional support and compassionate. That aid as a source of energy, inspiration for me throughout the period.

Date: 6-12-2013 **Sunny Gupta**

Regd no. 41100060

TABLE OF CONTENTS

List of Figure

Chapter 1

Introduction

1.1 Introduction

Web Service Security is an important part of Computer Sciences and Technology. Many IT Companies use the web services for the development of an application. Moreover, Many IT professionals worked on the security of the web services. These IT professional having a basic level of knowledge of Web Services, related security issues, and the standards of security which always emerges. They may work intelligently with application developers to securely build and implement web services. Most of the time people do often face the problems related to the web services such as if a person knows the path of the web service that the user need to access then the person can easily get to know about the functionality of the web service which may results in the hacking of the website as well as the user's personal data which is very dangerous process [1]. By using the web service path the user can get to know about the loopholes in the website and by using that loopholes the user can easily exploit the website and can hack that website.

For e.g. : if any bank asks the user about his banking detail to access any service of the bank then a hacker can get the secure information of the user using the loopholes in the web service which in results allows the hacker to get to the full access to the user account[1]. This is the major reason for which still the most of the user often feel hesitate to use the internet banking or doing any online transactions.

1.1 Web Services

With the help of the Web Services we can easily transfer the XML Data which contains any information across the different systems. The format in which the data is coming as the out from the web services is of xml type/format. The main bridge which is used to transfer the data from the client to server or vice versa is a protocol which is known as soap. To create the applications the web services are very helpful [2]. The main application of the web services

are that we need to create the web services only once and once we create these web services we can use these services on any platform and on any application[3].

Web services for the .net provides the communication for the applications of the xml which is asynchronous by nature which allows us to operate them on the communication framework of .net. The main purpose of the existence of the web services are that these are not dependent upon the local system of the user and are generally based on browser [3]. With the help of the web services we can convert our application to the web application.

For that we need to publish our web service using the IIS then link this service to the application and the application which wants to use these service needs to call it with help of get and post method.

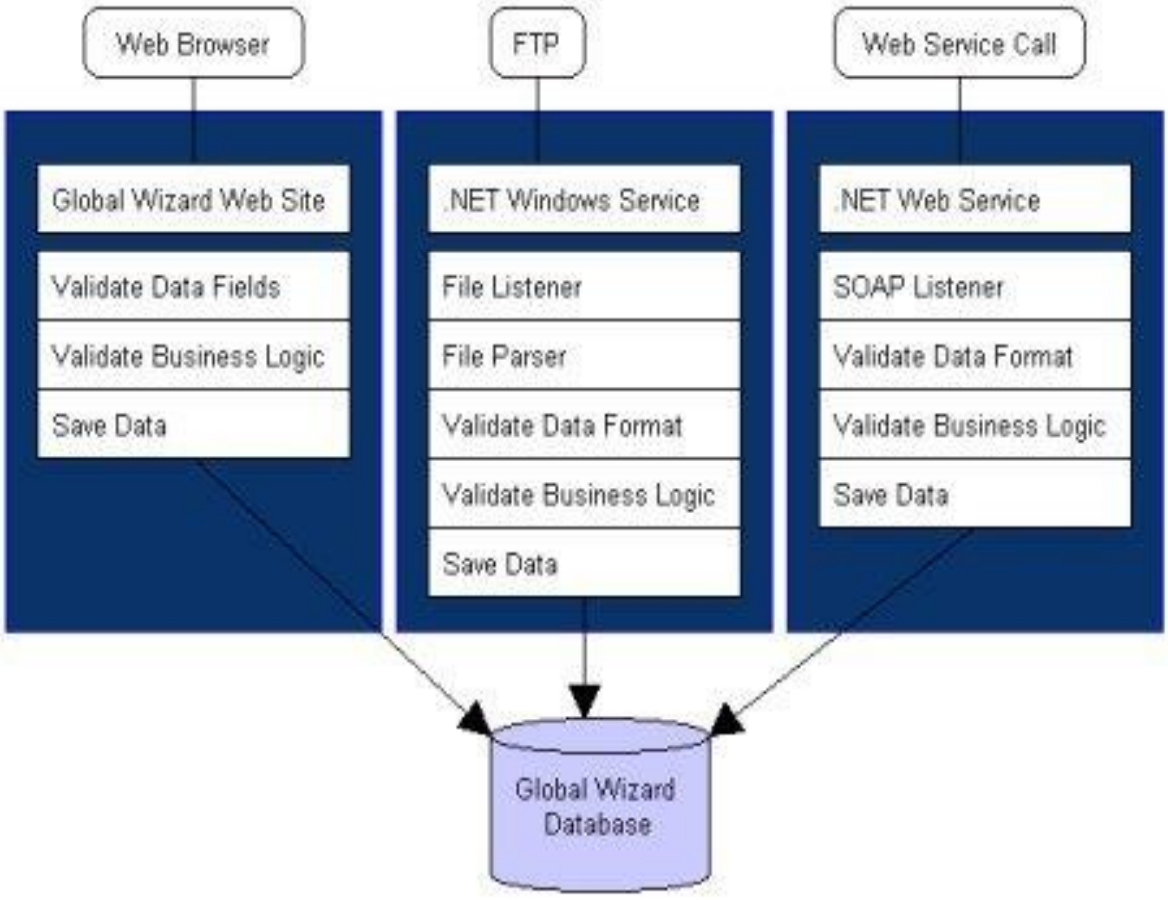

Fig. 1.1 Working of the Web Service

There are two kind of web service responses which are mostly used by the web site developers these are a) Json b)Xml [5].

With the help of these two kind of responses the web services transfer the data through internet from the user these two kind of responses considered as the fastest way to travel the data over the internet but along with the advantages of these two responses the disadvantages are also there the main disadvantage of these responses is that these are associates with the web services which are not so secure so by getting the hold on the web service any user can easily get the information which is contained either in json or xml. Moreover the structure of these two responses is so simple that the user can easily get the information about the particular filed by reading the detail inside these responses.

1.2 Web Service Architecture

The server which were before the web services provides some features which can be called by the user [3]. These functionalities acts as the bridge between the server and the client. The main three components of which web services exists are:

- There is a broker which acts as a look up between the provider of the service and the requestor of the service.
- The Provider of the service is that who publish its services to the broker of the service.
- The requestor of the service is that who asks the broker of the service about where to find the suitable provider of the service and binds itself to the provider of the service [3].

  Following diagram show the relationships between web service and components:

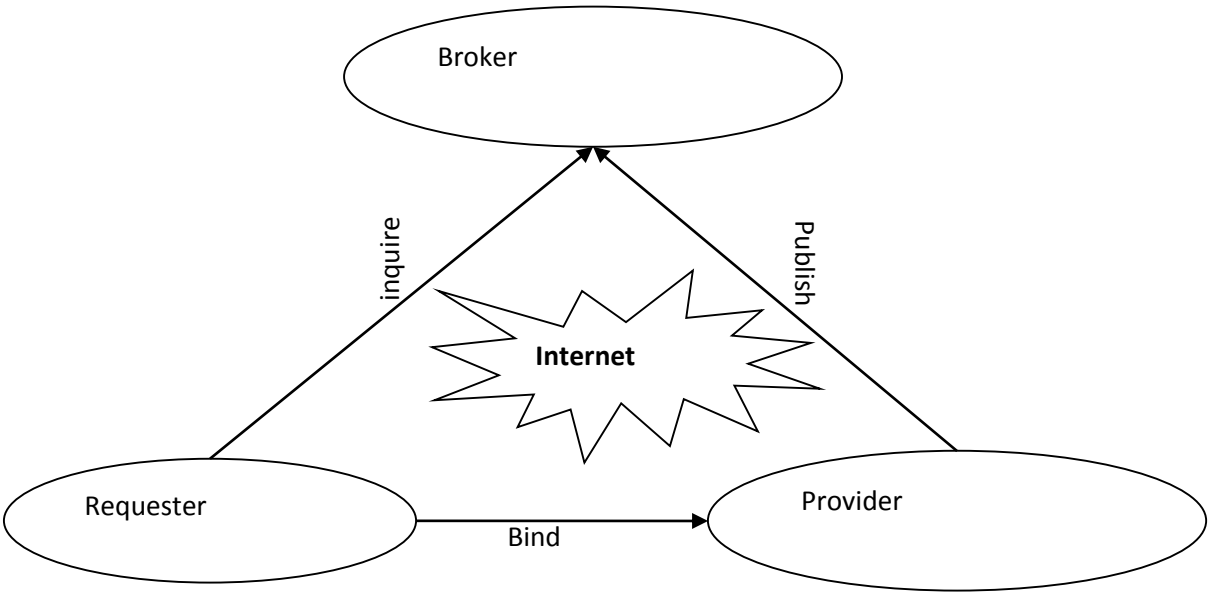

Fig. 1.2 Architecture of the Web Service

Web service has the following Layers:

On the Top of the protocol of the HTTP web services uses xml which allows it to gets no problem related to the firewall. Because as we know generally firewalls do not block the http protocol. If we carefully check then we will came to know that when web services do not need to use the http instead of http the use of SMTP and ftp is considered [3]. Xml is the format which is widely accepted for transferring the data and its semantics.

Web Services stack which consists of the layers of web services consists of the following parts:

• XML (Extensible Markup Language).

• SOAP (Simple Object Access Protocol).

• WSDL (Web Services Definition Language).

• UDDI (Universal Discovery Description Integration).

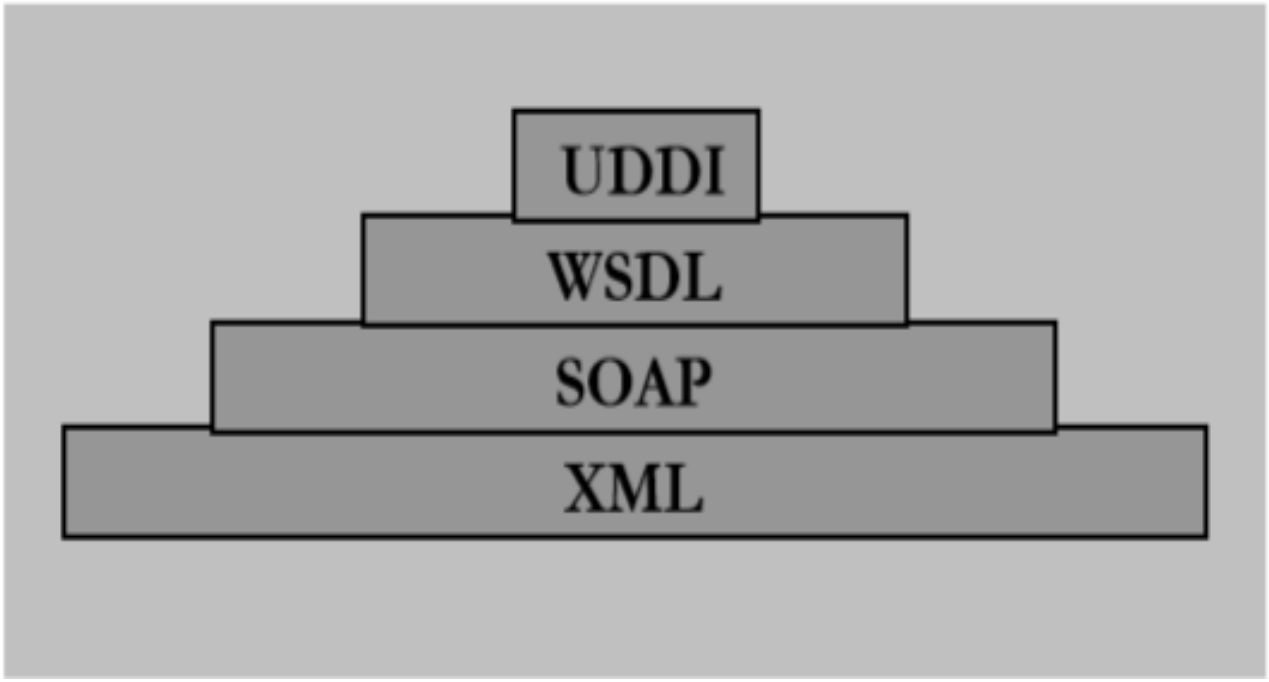

Fig 1.3 Layer of Web service

The figure which is above by no means can be considered as complete. The layers shown in the figure use to build a foundation which allows us to develop the web services.

The architecture of the web service includes the four steps which are as following.

1.2.1 Service Processes: This part includes the web services in the collection and mainly includes the thing which is known as the discovery because it allows to search and find the particular service from the collection of services.

1.2.2 Service Description: The most highlighting feature of the web services is that these are self-describing which means that once we have located the web service then we need to ask it to define itself and which will give you the response that which operations it supports and how we can invoke that operations.

1.2.3 Service Invocation: The term invoking the web services means that sending and transfer the messages from the client to the server and in this process the soap tells the client about the format of the request and the response of server to the request.

1.2.4 Transport: The messages which are sent by client to the server are in the form of the http architecture and to use the web pages this architecture is used.

The layers of XML in detail

SOAP

As we all know that the web services used to run in the different environments which means that to use the web services we need such a protocol which is independent of any environment and the protocol which have these features is the SOAP.

The main feature of the SOAP is that the semantic of any application is not defined by the SOAP itself. The Examples of the semantics includes such as garbage collection [4]. The SOAP provides a mechanism which is used to encode the data within the modules which is to express the semantic of application.

There is a tag named as the envelope at the root of the SOAP messages. There are two types of elements in the ENVELOPE which are:

- An optional header.
- A body.

Differences in SOAP versions

There are two versions of the SOAP which are: 1.1 and 1.2 and both theses versions follow a standard named as World Wide Web Consortium [5]. We can deploy the web services which does not support only SOAP 1.1 but also SOAP 1.2. The Changes which are made in the SOAP 1.2 are minor as well as significant.

The SOAP 1.2 includes a lot of changes as compared to the SOAP 1.1. The most important differences between the Current versions of the SOAP are as below:

The Changes which has been made in the SOAP 1.2 and those who are significant are as follow:

- SOAP 1.2 is based on the XML set of Information as compared to SOAP which is based on SOAP 1.1 XML.

- These is the facility in the SOAP 1.2 which allows it to define the transport protocols officially until the vendor conforms the framework to be bind. As we all know that the http is ubiquitous which not much reliable in any sense as compared to the transport.
- The SOAP 1.2 comes with the more specific definition of the SOAP processing which removes many ambiguities which results in the interoperability errors in the absence of the interoperability of the web services profiles [2]. The main objective of all these things are to remove the interoperability from the different vendors which uses the SOAP.

Specification Assertion and the Test Collection is the fourth document.

There SOAP 1.2 includes a lot of changes in terms of the syntax. It also provides the clear definition of the semantic from those which describes in the SOAP 1.1.The primer document of the SOAP 1.2 describes as well as lists the changes in the syntax [1].

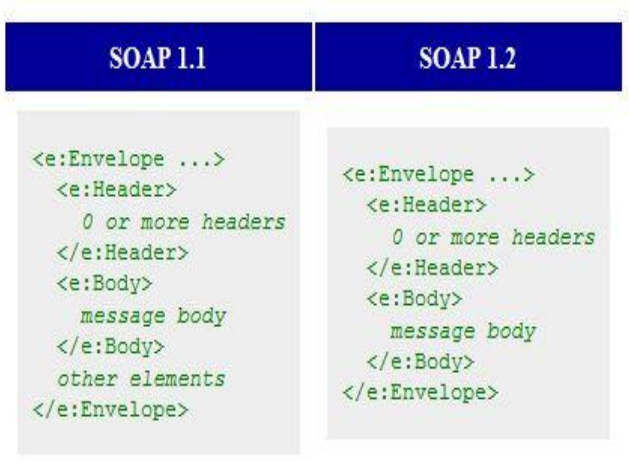

Fig 1.4 Different version of SOAP Architecture

1.3 Process to implement web service in an application:

Firstly we develop a service in asp.net and test all the services. In a second step we can host the service on IIS server. This server handles the request of each service call. We can use the server path to get service response in an application.

1.4 Security:

The main fundamental of security is for protecting Assets. Assets may be any kind of database, Items, Operations in the application or they may be less solid (tangible). Mainly security is a path not a destination for an organization [5]. As we analyze our infrastructure and application, we identify potential threats and understand that each threat presents a degree of risk. Security is about risk management and implementing effective countermeasures.

1.4. 1.Security Foundation

Security based on the following elements:

- **Authentication**: Authentication is basically the question of Who are you? It is used for identifying the clients of your application and services. Authentication in simple language is the process by which the user get the access of any service for which they are registered. The authentication is really a very important part in the web because this is the step which restricts any user to get an anonymous access on any web service or any service which increases the security and integrity in the web sites [7]. Example: Login process of any application is an **Authentication** Process in which the user enters his/her credential in order to access any service related to any web site. The Authentication is now the part of every website so that the user can maintain his/her personal data without the intervention of any outside user.
- **Authorization:** Authorization is basically the question of what can you do? It is to govern the resources and operations that the authenticated client is permitted to access. The authorization step gives the user limited access of the website or you can say the user can only access those service which are allowed by the role in which he/she is assigned [4]. Example: In an application many module are available. To give the access

of module user wise is an authorization process. This authorization used for include files, databases, tables, rows, and so on. The next example is so common in the web which is to access the free and the premium (paid) account [9]. The users who are registered under the free account are only allowed to access the few services which are provided by the website as free services for the free users which allows the user to get the trail run of every service in the website with few limitation and if the user feel that the services are really good for him/her then he/she can access the services full functionality by purchasing the services from the website.

- **Auditing:** Effective auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. Which help in the deduction of the transaction failures and the transaction deadlock such kind of the security measure are usually taken in the field of the e-Commerce where such issues really important for the customer as well as for the supplier [12]. For example, in an e-commerce system, non-repudiation mechanisms are required to make sure that a consumer cannot deny ordering 100 copies of a particular book.
- **Confidentiality:** Confidentiality is related to as privacy, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Confidentiality is the process which makes sure the user that his/her personal data cannot be viewed by any other personal without using the credentials of the user which increases the confidence in the user to use the internet services for each and everything where it is required to share the personal information of the user.
- **Integrity:** Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes. Moreover, Integrity insures that the data secured and nobody has done any with this data [10]. This kind of process is really important in the field of online chatting where the user talks with the other personal so they do not want the any modification in the messages which they send which results in avoidance of any kind of misunderstanding between the users.

- **Availability:** From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with **denial of service** attacks is to crash an application or to make sure that the application is sufficiently overwhelmed so that other users cannot access it [8]. In the denial of service attack the hackers sends the multiple request to the web server of the website so that the server remain busy to process the fake request sends by the hacker and the authenticated user cannot access the system due to the server busy state.

1.4.2 Threats and Vulnerabilities in the Security:

- **Threat**: A threat is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to your assets. The threat can be occurred due to two reason : i) Intentional ii) Accidental [14]

  First of all the Intentional Threat which is the intelligent work done by any individual cracker with the intension to exploit the system or this work done by any official hacker of the company to know the loopholes in the system.

  On the other hand the Accidental threat results due to the malfunctioning of the computer or due to the natural disaster such as earthquake etc.

  There is the different types of the categories of the threats such as:

  a.) **Spoofing of User Identity:** In this the user information can be gathered by a threat and can be used for the unwanted purpose.

  b.) **Tampering:** In this the user information can be tampered with the help of the threat in the system.

  c.) **Repudiation:** In this the information related to any thing is changed which might be the secure information of the any user.

  d.) **Information Disclosure:** In this the private information of the user can be disclosed or the data can be leaked from the user personal system.

  e.) **Denial of Service:** Denial of service means to prevent the authorized users to access the services by keeping the server busy with fake requests and at the end makes the network breakdown.

  f.) **Elevation of Privilege:** In this any bug in the system is exploited to gain the unauthorized access on the system and use the system for unwanted purpose.

With all these categories of threat there is categories of risk is also associated with it which are: Damage, Reproducibility, Exploitability, Affected User and Discoverability.

- **Vulnerability:** A vulnerability is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. Weak input validation is an example of an application layer vulnerability, which can result in input attacks [19]. Vulnerability is possible with the help of the combination of the three thing First of all a system flaw and second is an attacker get the access on that flaw and the third is the capability of the hacker to exploit that flaw. The vulnerability can be classified in different categories which are:
  a.) **Hardware:** The vulnerability in the hardware can be happen due to the one of the following reasons which are: humidity in the hardware, dust in the hardware, susceptibility of soiling and due to the storage which is unprotected.
  b.) **Software:** In the software the main reasons of the vulnerabilities are lack of testing of the software and also the less audit trail in the software.
  c.) **Network:** In the networks the main reasons for the vulnerabilities are the communication lines which are not protected and the network architecture which is not secure.
  d.) **Personnel:** This type of vulnerabilities are the result of recruiting process which is inadequate and also the security awareness which is not up to the mark.
  e.) **Organizational:** The main reasons for such vulnerabilities are due the insufficient regular audits, Lack of plans which needs to be regular and very important one is the lack of security.

- **Attack:** An attack is an action that exploits vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application, or flooding a network in an attempt to deny service.
  Types of Attack:
  a.) **Active Attack:** The attack which includes some changes in the data stream or produces some false data stream is known as the Active attack. The Active attack

further can be divided into four categories which are denial of service, modification of messages, replay and masquerade [20].

i.) **Masquerade:** In this type of attack one person acts to be the other. For example the authentication detail of the user can be captured after the valid authentication by acting to be another person.

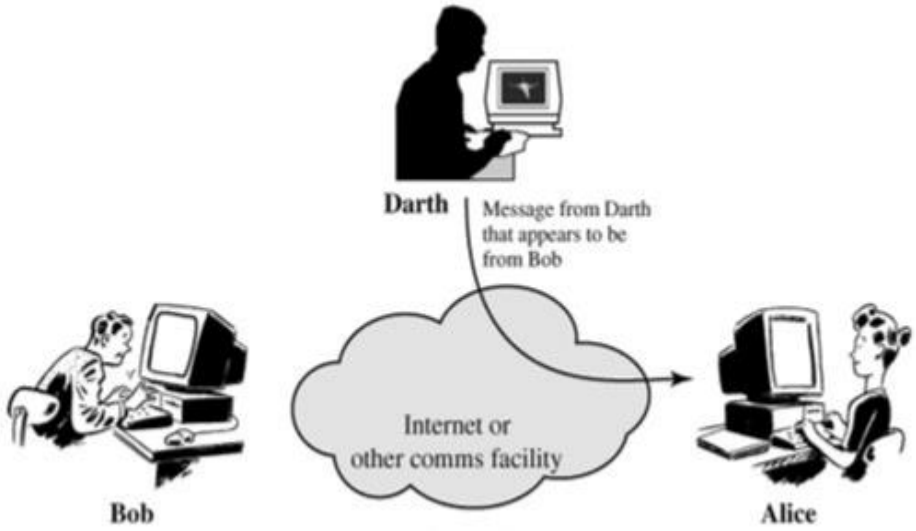

Fig 1.5: Masquerade

ii.) **Replay:** In this attack the data unit is captured and then with the help of the retransmission of the data an unauthorized effect can be generated.

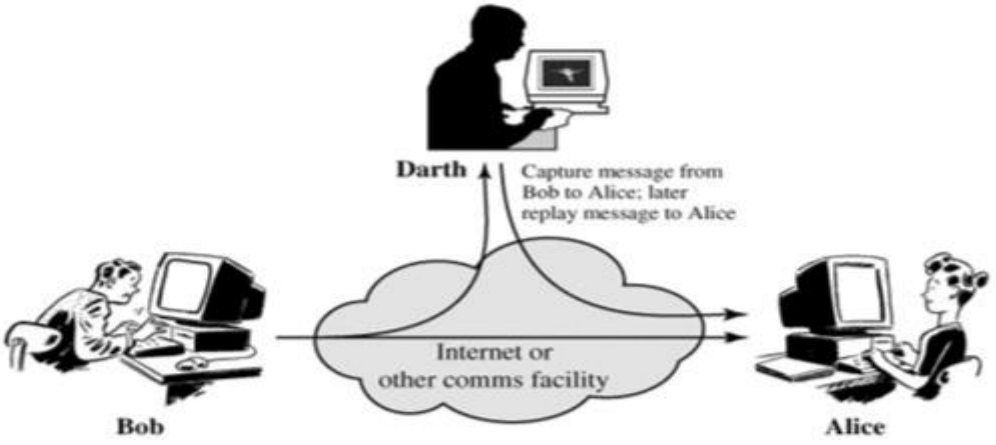

Fig 1.6: Replay

iii.) **Modification of Messages:** In this the content of the messages has been altered or the messages can be delayed or reorder in order to produce an effect which is unauthorized.

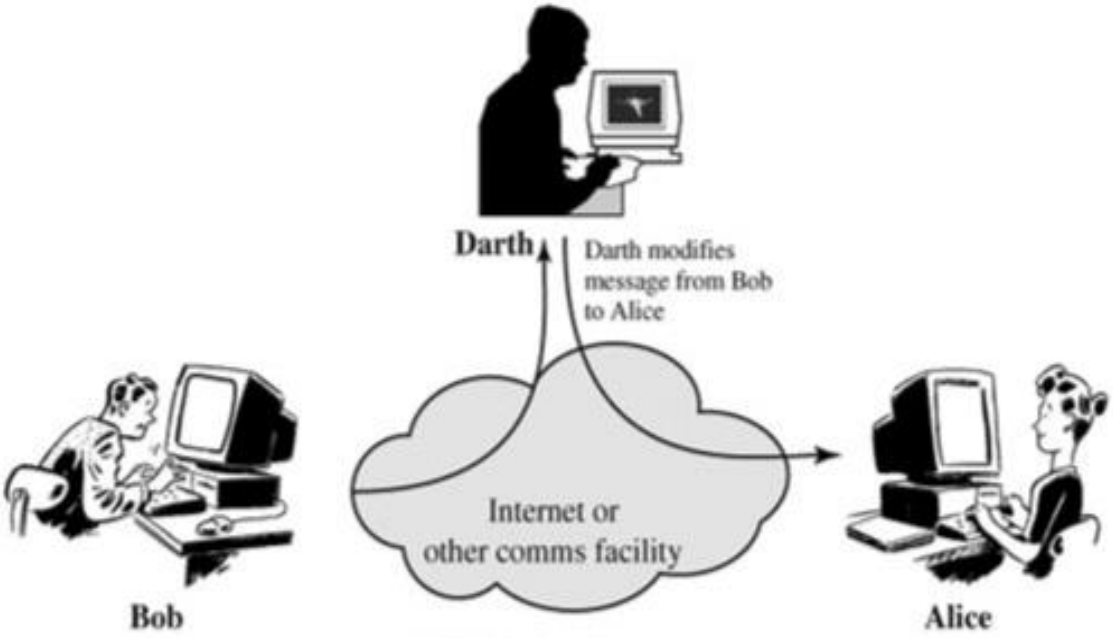

Fig 1.7: Modification of Messages

iv.) **Denial of Service:** This type of attack prevents the user from the normal use of the services of the communication.

Fig 1.8: Denial of Service

b.) **Passive Attack:** In the passive attack the main goal is to get the information which is being transmitted either by use of eavesdropping, monitoring or transmissions. This type of attacks are categorized into two parts which are:

i.) **Release of Message Content:** In this attack the messages content which are transmitted with the help of the electronic mail, telephonic conversation and transferred file has been read [20].

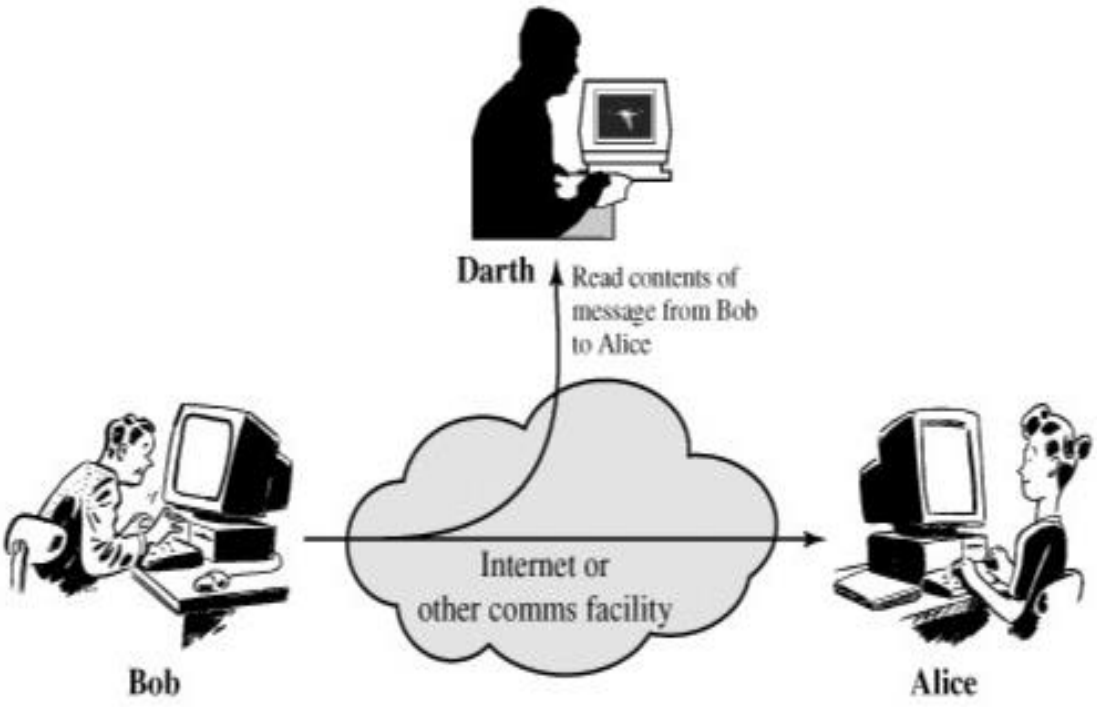

Fig 1.9: Release of Message Content

ii.) **Traffic Analysis:** This kind of attack involves in getting the information related to the length of the message and the location of the communication host which allows the attacker to know the nature of the message that is being exchanged even on the encrypted messages.

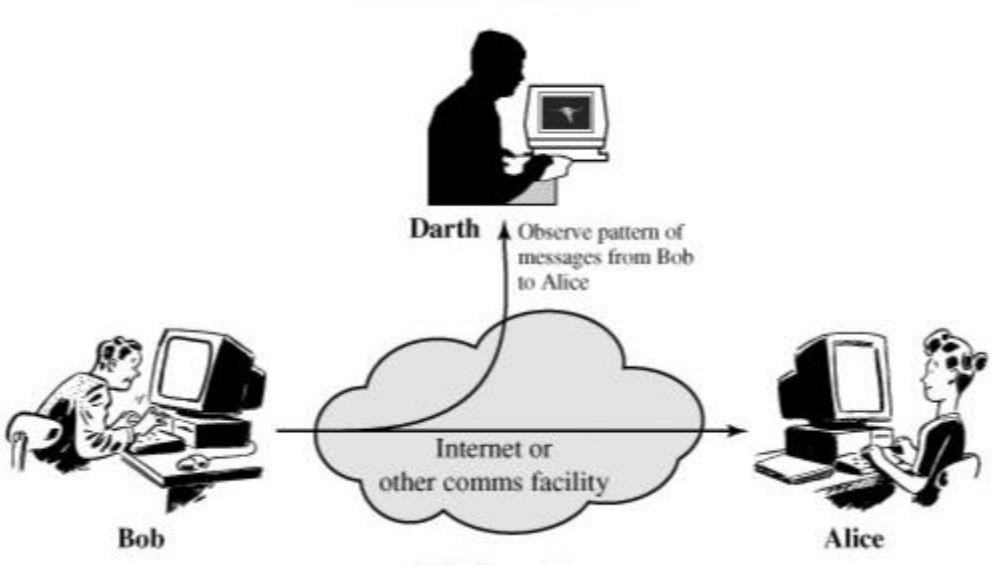

Fig 1.10: Traffic Analysis

Moreover the passive attacks are very difficult to detect because these types of attacks does not alter the messages it just only read the messages which is very difficult to detect. Although encryption prevents passive attack but still it cannot detect the passive attack.

1.5 Security in web service:

Web Services security discussions are all over the media these days, why is that? To security-minded people like us, the answer is probably obvious. After all, we just explained that SOAP is a standard to allow others (other users, systems, servers, objects etc.) to execute code on a system. What we've just described is in fact every hacker's dream. This is a story that seems to keep repeating itself in the technology field. In application developers' headlong rush to implement new technology, functionality, and openness guess what they forgot to think about? That's right- security! As often happens (developers are often focused on functionality, proper operation, interoperability, and deadlines) security has become an afterthought [16] , an add-on to Web Services, rather than being built in from the ground up.

1.6 Advantages of Web Services:

1. As the web services use the standard XML language these are the platform independent and the language independent [5]. Which means it does not matter whether my program has been built using C++ in Windows and Worked in the Linux.

2. The major advantage of the web service is that it uses the http for transmitting the messages across the internet and most of the internet proxies do not mess with the http.

1.7 Disadvantages of Web Services:

1. Overhead: The data which is transmitted with the help of XML is not as efficient as is transmitted by the binary code for which the most of the real time systems not use the web services [5].

2. Lack of Versatility: The versatility in the web service is very less and it allows very simple and basic form of service invocation.

1.8 Limitations of Web Service Security:

For Example if a user develop an android application for the university system, If the user decodes .apk file and know the service path then the user can easily assess the server services without making any effort. Or any web service which is deployed on server can be seen by the user by posting the address of that service in the address bar of its respective internet browser. Asserting further, if the exchange of messages between the service provider and the consumer are frequent then the overhead of XML Sig and XML ENC is significant [17]. In Addition to this, in web services the merging of the several xml schemas for increasing the security in the web services causes the dependencies issues on the different versions of the library which is difficult to manage in application layer. If the web services uses the CBC mode of encryption and decryption and apply this scheme without verifying the checksum then this implementation is likely to be vulnerable to padding oracle attacks.

1.9 Kerberos Security Model

1.9.1 Kerberos Introduction

Kerberos is the third party authentication protocol which means that for the authentication purpose server and client has to rely on someone else which will authenticate both the server and client. Kerberos authentication is based on symmetric key cryptography which means that the client and server will share a single key for encryption and decryption. In this Client proves it by encrypting the message with the key and the server proves it by decrypting that message. After this, Server again encrypts the message and sends it to the client again [22]. Kerberos authentication relies on the central server which is called key distribution center (KDC) which provides all the keys. KDC Issues the ticket granting ticket to the client which want to access a resource from the server. Kerberos authentication is used in various places but the biggest achievement of the Kerberos authentication is that it is used as default authentication in Windows XP and Windows 2000. The only limitation in the Kerberos is the scalability as it is very important in this modern era where everything is expanded day by day along with the usage of internet. However, Kerberos can achieve the Scalability with the help of public key cryptography.

1.9.1.1 Working of Kerberos

The Kerberos authentication is done in three major steps:- Initial Ticket Granting Ticket is acquired by the Client. Client uses the acquired Ticket granting ticket to get the ticket to access the resources from the server. The client use the ticket to access the resources from the server.

1.9.1.1.1 Initial Ticket Granting Ticket (TGT) is acquired by the Client:

To get the TGT client has to go from several steps which are as below. First of all the user logs in to the client machine using the username and the password. After this, client encrypts the password and saves it. Asserting further, Client sends KDC a message requesting the credentials for the TGT service along with the authentication message and user's encrypted password. Authentication message includes client name, network address and timestamp. KDC compares the encrypted password with his master copy to make sure that it match (it is done by the authentication server in KDC) so that the client can be verified after the password matches, KDC also compares the timestamp and it should be within 5 minutes of its own time.

If everything matches then KDC generates requested credentials for ticket granting ticket service by creating the logon session key and encrypt it with user's key [13]. KDC also creates another credential which contains logon session key and encrypts it with its master key. Moving further, KDC sends both these credentials to the client where client decrypts the logon session key with its encrypted password and stores the logon session key along with TGT in its ticket cache.

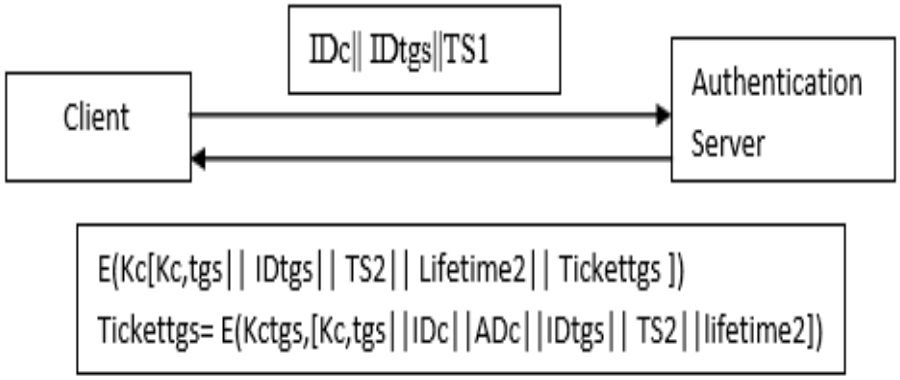

Fig. 1.11 Authentication Service Exchange to obtain ticket-granting ticket

1.9.1.1.2 Client uses the acquired Ticket granting ticket to get the ticket to access the resources from the server

In this step, client demands the ticket from the KDC to access the resources from the server, for this client present its TGT, resource name and authentication message which is encrypted by the client with the help of the logon session key. The KDC Decrypts the TGT using its master key and extracts the logon session key. This Session key is then used by the KDC to decrypts the message from the user. If it matches then user is verified. After this KDC creates the service session key for the client so that it can be presented by the client to the server whenever client requests the resource from the server. This service session key is encrypted with the logon session key of client. KDC Also encrypts this service session key with server's master key. This all is done by ticker granting service in KDC. After this, KDC send both the

credentials to the Client which decrypts the service session key with the help of the logon session key and stored the Service session key along with tickets in its cache.

The server decrypts the service session key using its master key and with the help of this service session key decrypts the message sent by the user, after decrypting the authentication message server gets session ticket and compares the timestamp the client put on the time of request with its own time and check whether it is within 5 minutes of its own time or not. Server then encrypts the timestamp in the session ticket with service session key and sends it to the client [14]. The client then decrypts the message and compares it with its original timestamp. If it matches, then user gets authenticated and gets the access on the requested service of the server.

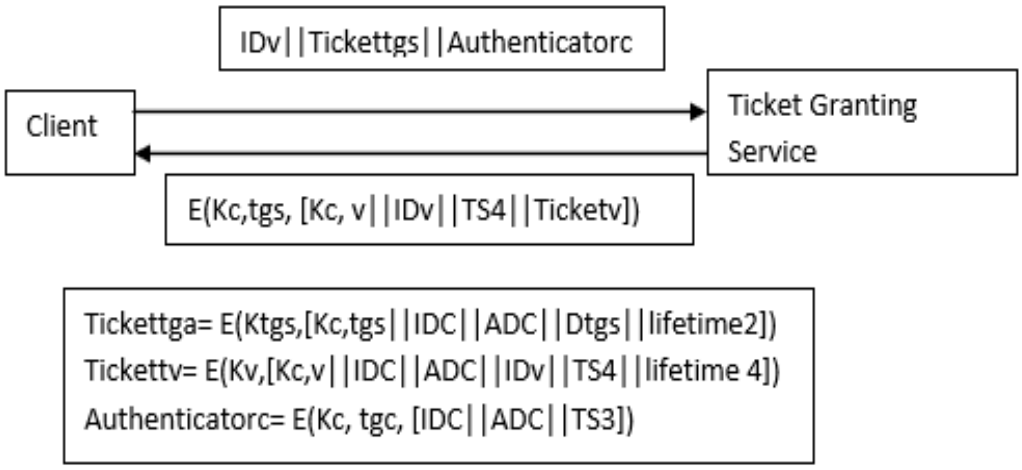

Fig. 1.12 Ticket-Granting Service Exchange to obtain service-granting ticket

1.9.1.1.3 The client use the ticket to access the resources from the server

This is the final step in the Kerberos authentication and it involves the following steps:

- The Client in this step sends the session ticket along with the authentication message and encrypts it with service session key.
- The server decrypts the service session key using its master key and with the help of this service session key decrypts the message sent by the user, after decrypting the authentication message server gets session ticket and compares the timestamp the client

put on the time of request with its own time and check whether it is within 5 minutes of its own time or not.

- Server then encrypts the timestamp in the session ticket with service session key and sends it to the client.
- The client then decrypts the message and compares it with its original timestamp. If it matches, then user gets authenticated and gets the access on the requested service of the server.

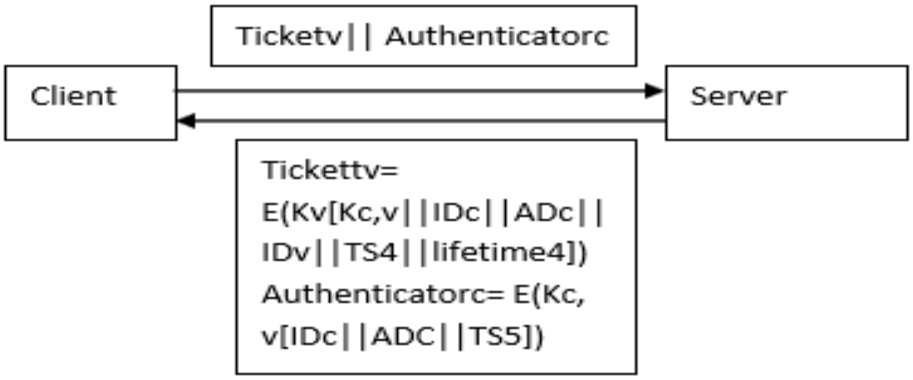

Fig.1.13 Client/Server Authentication Exchange to obtain service

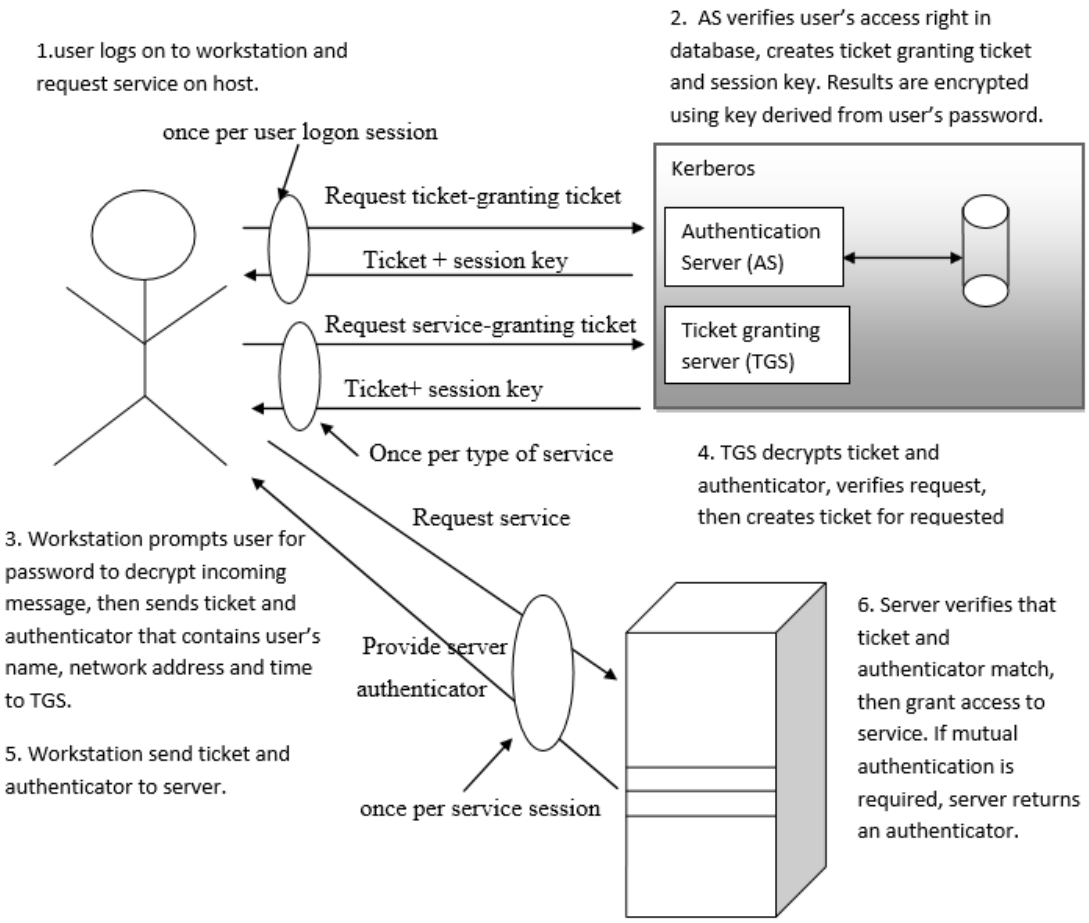

Fig. 1.14 Overall Working of the Kerberos Authentication

1.10 Location Based Services:

Location based services are such services which controls the features using the data gathered for the location. The Location based services has an important role in the social networking. Moreover with the help of the global positioning system the location based services has also an important role in the mobile devices and the role is becoming more important with the expansion of the tablets and the smartphones as well [19]. The Location Based Services includes a lot of thing such as locating the near ATM, Hotels, abode of a friend etc. This Services also includes the vehicle tracking and parcel tracking services. These type of services also used in the mobile commerce where the special discounts has been provided by

the companies to the customers based on the current location of the customer such the shipping charges provided by the companies for the locations.

1.10.1 Locating Methods:

There are different types of methods which are used to get the data of the location and provide the service to the user about the location according to his/her need the methods which are used to do this are as below:

1.10.1.1 Control Plane Locating:

In this method the location of the user can be determined by the radio signal delay from the closest mobile tower for those user who has the mobile phones without the feature of the global positioning system [17]. This way of locating the user location is very slow because it uses the voice control signal. This type of method follows the following factors to be met in order to get the location of the user accurately:

- Lowest possible cost.
- Minimal Impact on the network and equipment's.
- The Requirement should be accurately coordinated which are determined by the relevant service.

1.10.1.2 GSM Localization:

This is another way to find out the position of a mobile phone. In this method the position of the mobile phone can be determined through the mobile site. The location of the mobile device can be determined using the time difference of arrival.

1.10.1.3 Self-Reported Positioning:

This method is the cost effective method from all the above which uses to track the player instead of track all. This technique uses the augment reality to find out the location of the user. In This technology the players where given the map and they were ask to mark their location in the map this technique was also known as the check in.

1.10.1.4 Others:

The other includes the rest of the techniques which are used to find out the location of the user which includes the nearby location based services this uses the local range technologies such as the Wireless LAN, Bluetooth and infrared technologies to match the service which is near to the user [14]. This type of technology allows the user to access the information based on their surroundings.

Another technique which do the same functionality is the search of the deep level network of telecom which gives us the accurate and the quick response of the geographical coordinates of anybody's mobile number.

1.10.2 Location Based Services Applications:

There are lot of applications associated with the location based services such as:

- Find out the people in the map which is displayed on the mobile phone screen.
- Mobile Advertisement based on the location.
- Mobile Commerce offers based on the location.
- Games which are dependent on the location of the user.
- Get the information about the restaurants and the hostel according to the location.
- Social events recommendations in the City.
- Alters related to anything which includes the traffic problem in the area.

Chapter 2

Review of Literature

Mr. S.K. Pathan, Mr. S.N. Deshmukh, Dr. R.R. Deshmukh(2009) presented a paper "Kerberos Authentication System –A Public Key extension" which describes the importance of the public key encryption in the today's world. This paper describes that the Kerberos is the secure and reliable in terms of the authentication protocols, But this approach is mainly depends upon the secret key encryption technology and to be able to authenticate the large number of users on the internet it may use the general-purpose authentication protocol. To make this approach to be able to authenticate the large number of the users several proposals has been developed all of which focuses on the addition of the public key cryptography on the various stages of the Kerberos, but this approach has one drawback that is the computational requirement of the public key cryptography is more than the secret key cryptography which results in the decrease of the performance. To overcome this drawback this paper introduced the alternative approach of the public key cryptography. [14]

Alin COBÂRZAN(2010) presented a paper "Consuming Web Services on Mobile Platforms" which describes the use of the web services in the web and also the benefits of using the web services in the Mobile Devices. The paper also introduced the challenges that we need to face when the implementation of the web services will be done on the mobile devices which are consumes the low resources and connected through the unreliable wireless connections. Moreover, this paper also focuses on the communication architecture which is based on the XML for the transfer of messages from the mobile devices to the external middleware component, this middleware component acts as in the same way as acted by client and server with addition to resolve the problem of the requests to the web service. [3]

Li Jiang, Hao Chen, Fei Deng(2010) presented a paper "A Security Evaluation Method Based on STRIDE Model for Web Service" which describes the advantages of the webservice such as the webservices are the self-descriptive and loosely coupled. But, this paper also focuses on the problem to evaluate the webservice security. To overcome and solve this problem this paper has introduced a model named as "Stride". By using the properties of the web services and the

threat evaluation method of the stride model this paper provides the web security evaluation model which really helps the users to create the threat modelling and evaluating the degree of safety for the web service security. In many systems the experiments shows that it provides the valuable check to evaluate the threat and the security vulnerabilities of web service security and optimize the system security. [12]

Xiaohong Li, Yan Caoy, Zhiyong Fengz, RanLiux(2010) presented a paper "Web Service Security Analysis Model Based on Program Slicing" which describes analyses model of the web sevices which is based on the program slicing whose main purpose is to find the already existed critical information and disclosure of the vulnerabilities, mainly the those vulnerabilities which is in the web services net and which eventually improves the protection in the critical information. This paper uses the source code and slice that to obtain the interface information flow and after this critical information has been checked to see whether it is disclosed through the interface information flow. To check the Vulnerabilities proliferation two web services has been used in which the critical information has been transmitted and disclosed then based on this a security report has been generated. [18]

Amit Kushwaha , Vineet Kushwaha(2011) presented a paper "Location Based Services using Android Mobile Operating System " which describes the importance of the palmtops and the mobile phones which almost replaced the laptops even for the computational work. This paper also described the need of the people to know about the location where they are roaming which can be only done with the help of the location based services. The paper creates such services which includes the information regarding the location in which the user visits to make sure he or she do not need to take any guide along where the user is going and moreover the user need not to carry the laptop in order to access the services related to location the user just to carry his mobile phone to access the services and know about the location in deep. [4]

Chi Po Cheong,Chris Chatwin and Rupert Young(2011) presented a paper "A New Secure Token For Enhancing Web Service Security" which introduced the new secure web token to increase the security in the web services which provides the integrity as well as the confidentiality in the web services. As the most of the systems uses the service oriented architecture to implement the web services and uses the soap and xml to transfer the messages between the client and the server with the help of the HTTP protocol. The security become even more essential because the data is transferred on the public network that is on the internet and the location of the message sender is not authenticated which can be improved by the help of the token. [5]

Emam EL-Emam, Magdy Kutb, Hamdy Kelash and Osama S. Faragallah (2011) presented a paper "An Authentication Protocol Based on Kerberos 5" which implemented the some modifications in the Kerberos authentication protocol in order to overcome the drawbacks of the Kerberos protocol. The first modification which is describes in this paper is making the secret key independent from the user password which allows it to overcome the problem of weak password choose which can be easily accessed using the password guessing attack. Another modification which has been done in this paper is to control the life time of the realm using system key and for encryption use the triple DES and for the random number generator use the blum blum shub instead of saving the profile in the each instance of realm. [6]

Aditya Harbola,Deepti Negi and Deepak Harbola (2012) presented a paper "A New A3 Kerberos Model" which describes the importance of the authentication, authorization and the accounting in the today's world. This paper describes that the Kerberos can offer the authentication as well as the authorization but the accounting is not being provided by the Kerberos which is also very important. So this paper proposed the new technique which allows the use of the accounting in the Kerberos which allows the Kerberos to send the Kerberos ticket to the accounting server and the accounting server used to verify the user databases and the service providers and the ticker has the limited validity period. [2]

Hao Zeng, Dianfu Ma, Zhuqing Li, Yongwang Zhao(2012) presented a paper "A Policy-Based Architecture for Web Services Security Processing" which describes that as the internet usage has been increases day by day the web services becomes the first choice of the people to transmit the data between the internet and across the other websites specially in the field of the e-business, e- government and other fields. Which makes it even more important to make the web services more secure but there is no good method available to support the individual security requirements. So by considering this all need this paper comes with policy based architecture termed as PBA4WSSP for web services security processing. The policy based architecture provides the flexibility in the security of the web services and more over it provides the five security services which includes integrity, confidentiality, nonrepudiation, authentication and authorization. [9]

Manav Singhal, Anupam Shukla(2012) presented a paper "Implementation of Location based Services in Android using GPS and Web Services" which describes the advantages of the location based services to the mobile users to get the information about their current location and process the same data to get more useful information about the nearby locations to them. Moreover, this paper describes that in order to implement the locations based services the user must be required to call the web service which can be done if the user has the internet available in his/her mobile phone and also the phone has the feature of the Global Positioning Service which are easily available in all the android smart phones. In this paper the location based services has been provided to the user with the help of the Google web services and walk score API to provide the multiple services to the user based on their location. [13]

Nikos Mavrogiannopoulos, Andreas Pashalidis and Bart Preneel (2012) presented the paper “Security implications in Kerberos by the introduction of smart cards” which describes that the public key Kerberos which is based on the smart cards is flawed. If the user has access to the smart card of any user he/she can impersonate the user even after user access to the card is revoked. In order to remove all these threats this paper purposed the protocol which helps in fixing the properties which should be provided by the authentication protocols in order to better equipped with the flaws which are arises due to the usage of smart card. [15]

Wei Fu, Yingzhou Zhang, Xianting Zhu and Junyan Qian (2012) presented a paper "WSSecTool: A Web Service Security Analysis Tool Based on Program Slicing" which describe However, the damage caused by service security problems is becoming more and more serious nowadays. This paper develops a web service security analysis tool, WSSecTool, which is based on program slicing. This tool includes three modules namely slicing module, safety publishing module and testing module. Slicing module analyzes source codes of web service to generate method dependence graph (MDG). After MDG is generated, the tool slices MDG to detect the unsafe methods and the spread of them. Safety publishing module helps to hide unsafe methods to make them invisible to outer users after publishing. Testing module can test the services published by this tool to validate the correctness and feasibility of our analysis method. The experiments show that our tool is effective and practical. [17]

Chapter 3

Present Work

3.1 Scope of Study: The proposed system can be used in any application which requires the enhancement of security with less network cost and with more efficiency. The Proposed system mainly used for the web applications which requires top level security for their data with more efficiency. The scope of the proposed system is very huge this proposed system can be used in variety of purposes. The purposed system can be used in the all the applications which requires the internet and the security with effectiveness. The applications which uses the web services really required some sort of security so for all those applications which required the web service need the proposed system to be implement on their applications so the secure web services can be accessed by the user with more confidence on the application. Hence by considering these all facts the scope of the proposed system is eternal in the web.

3.2 Problem Formulation:

There are lot of issues in the web services because the web services are the self- defining. So if we know the url of the web service then we can easily find the methods which resides in the web services and it its self tells the how to invoke these methods. For example the web services in the ums can be hack if he user knows the URL of the web services and the hacker can get all the data of any student using his/her registration number but to avoid this issue ums make the user to fill its username and password for authentication on every page which is very long process instead of the proposed system which can be make the system much secure and also more efficient.

The proposed system focuses on the problem of increasing the efficiency of the Kerberos without compromises the level of security provided in the Kerberos authentication. Moreover, the proposed system along with the increasing the efficiency of the Kerberos system focuses on the reduction of the network cost.

3.3 Objectives: The objectives of the proposed system development is to introduce such a system on which the people can rely for the transferring of their secure data across the web with less network cost. The Proposed system uses the various techniques to achieve this objective which is described in the research methodology. But the main objective of the proposed system is to achieve the Kerberos authentication security with more efficiency and with less network cost. Asserting further, the proposed system also focuses on providing the security in the private system with almost 1/4 network. The proposed system targets to provide such a functionality to the users which can provide the users to use the more secure system with less network cost for the purpose of transferring of their secure data over the internet either from the personal computer or from the mobile devices.

By considering the importance of the usage of the mobile devices the proposed system also focuses on the implementation of the secure location based service through which the user can know each and every thing about the place where he wants to visit without worrying to take the guide along with him. The proposed system will provide the location based web services which will be secure with the help of the effective Kerberos security so that there is no possibility of getting the information altered by anybody.

3.4 Research Methodology: To achieve the above mentioned objectives of the proposed system uses the various steps which are as below:

3.4.1 Authentication: In this step, the user will enter his username and the password for the purpose of the authentication and access the resources of the system and also chooses whether to use the public system or the private system. If the user chooses the public system the authentication will be same as in the Kerberos but if the user chooses the private system and logging the system for second time then the proposed system will make the difference which as below. If the user selected the option to be as the public system then on the time of the authentication the proposed system will generate a token for the user with the specific time. This specific time is the in which the user can access the services on the server without any interruption but after this specific time the user needs to again submit his/her password if the user want to access the services of the server for the further time period. This reduces the risk of the system to be hacked by the any user who is working on the public system and makes the data to be secure because by submitting the password again to the web server for generating

the token again results in an application with low risk where the user is not using his own device to access that service.

3.4.2 Authentication Server: In the next step the authentication server will authenticate the user according to the username and the password provided by user if the user has been authenticated by the authenticated server then the authentication server will generate the session key. This is the key which will initiate the session for the user so that the user can access the services of the webserver in the session for which the session key has been generated.

3.4.3 Ticket Granting Ticket: In this step the session key generated by the authentication server is sent to the ticket granting ticket in this step the ticket granting ticket will generate the ticket for the user to access the resources of the server and encrypt it with the help of the session key and also encrypt the session key with the help of the user password. The two encryption steps has been implemented on this stage to insure that the data which is send by the ticker granting server has not been modified by any unauthorized user and the key remain unchanged so the user can access the services with the key as it sent by the web server.

3.4.4 Client: Now the Encrypted ticket and the session key is sent to the User Machine where the user first of all decrypt the session key with the help of his password after that the user uses that session key to decrypt the ticket which is used to access the server resources.

3.4.5 Server: The user now uses the ticket to encrypt his request to access the server resources and send this to the server the server decrypts the request of the user using the ticket and allows the user to access the requested service.

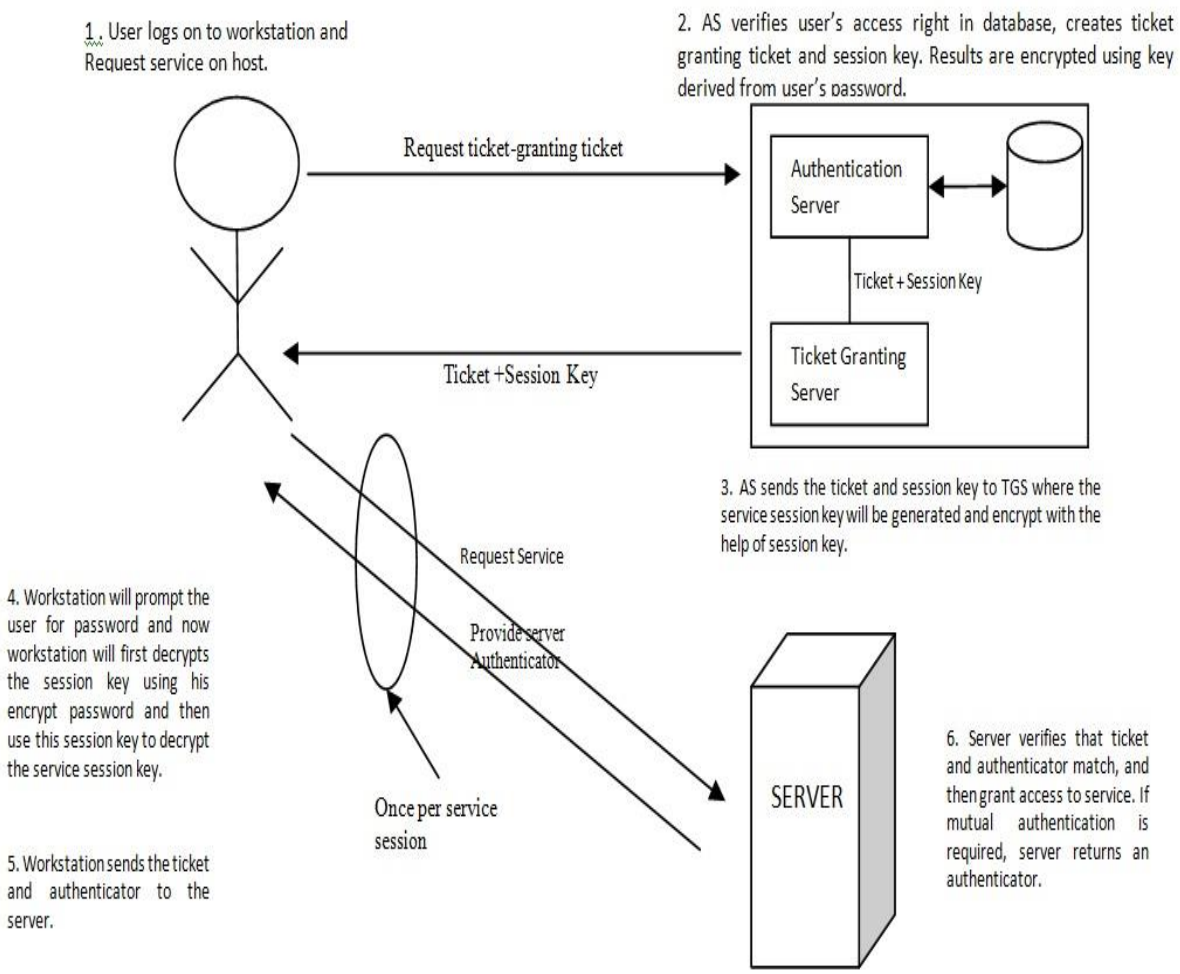

Fig 3.1 Proposed System for Kerberos Authentication

Chapter 4

Results and Discussions

The developed system secures the web services with the help of the Kerberos authentication with more effectiveness and less time whose performance can be easily seen when working with the public and private systems. As the Kerberos authentication follows so many steps in order to authenticate any request which starts from the generation of the token when the web request has arrived to the user followed by the request of the services which the user needs to access. This Request handled by the authentication server which is again send back to the server and ticker for the request has been generated whose authorization is checked by the ticket granting server and then send this request to the server if authorization is successful. But the proposed system uses the concept of public and private system which increases the authentication performance a lot because if the user chooses its system to be the private system then it is not required to send the request of the user back to the client system by the authentication server to the client machine for the ticket request the whole process can be done only at the time of the authentication where the authentication server directly transfer the ticket request of the user to the ticker granting server by doing this the time has been saved between the requests and more over the number of request also reduces which increases the performance of the system and reduces the network traffic.

The proposed system has shown the very encouraging result after the proposed system compared with different systems after the number of successful logins by the number of users. The results of the proposed system can be easily proved to be great by understanding the following example:

If the network cost to be considered to be 1 for every request and for the 100 users the network cost will be 100 for all users with their first request and if we consider the traditional Kerberos system then the network cost will be 600 for the 100 users because the network cost and number of requests are 6 for the traditional Kerberos authentication system. Moreover, the network cost is also same for the proposed system with the public system chosen by the user which is also 600. But the difference came only in the system when the user choses the system

to be as the private system for his use. If we considered there are 75% of the users who selected the option of private system to access the resources of the server then when the users logged in the system for the second time then the network cost will dropped to 450 which is a lot in the network related cost terms. This result and reduced network cost is shown in the following figure.

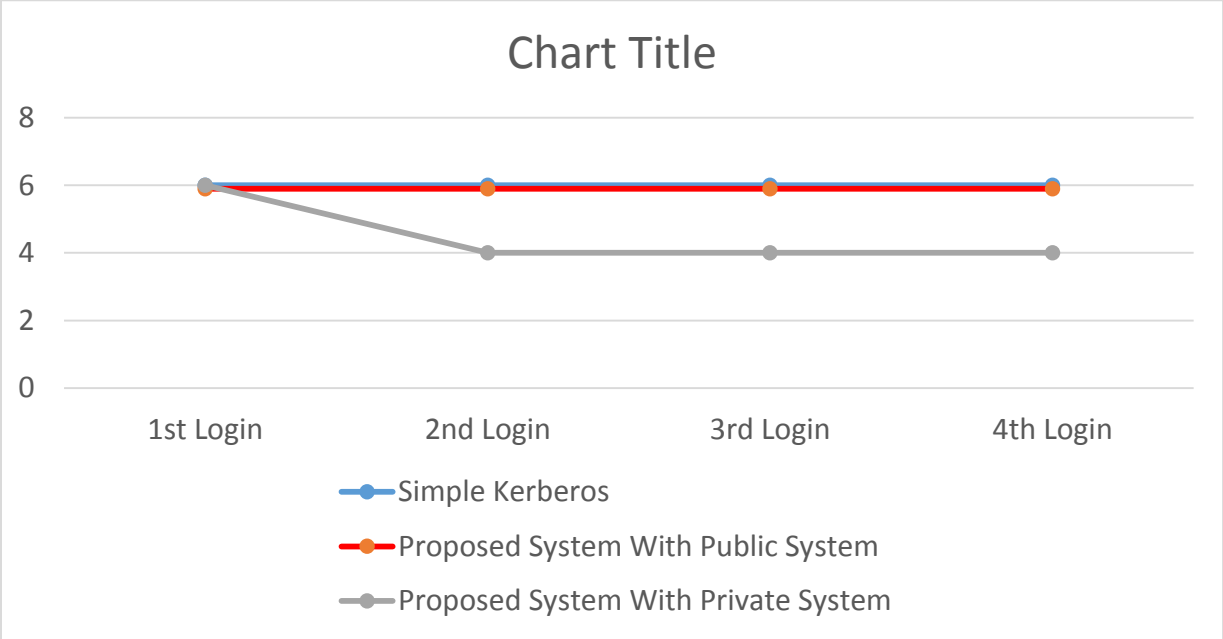

Fig 4.1: Network Cost Comparison of Different Systems

The results are more defined with more description in the bar chart which is shown in figure 4.2 in which the four type of systems has been explained which shows the different results according to the flow of the system and the steps followed by the different systems. The bar chart first of all illustrates the Kerberos authentication with every successful login of the user. The results are stable for the Kerberos authentication on each successful login by the user which is followed by the Kerberos system with all user choses the system to be public system which shows the same result as well but the proposed system with all users choses its system to be a private system shows the fluctuation and registered the minimum network cost of all the above systems.

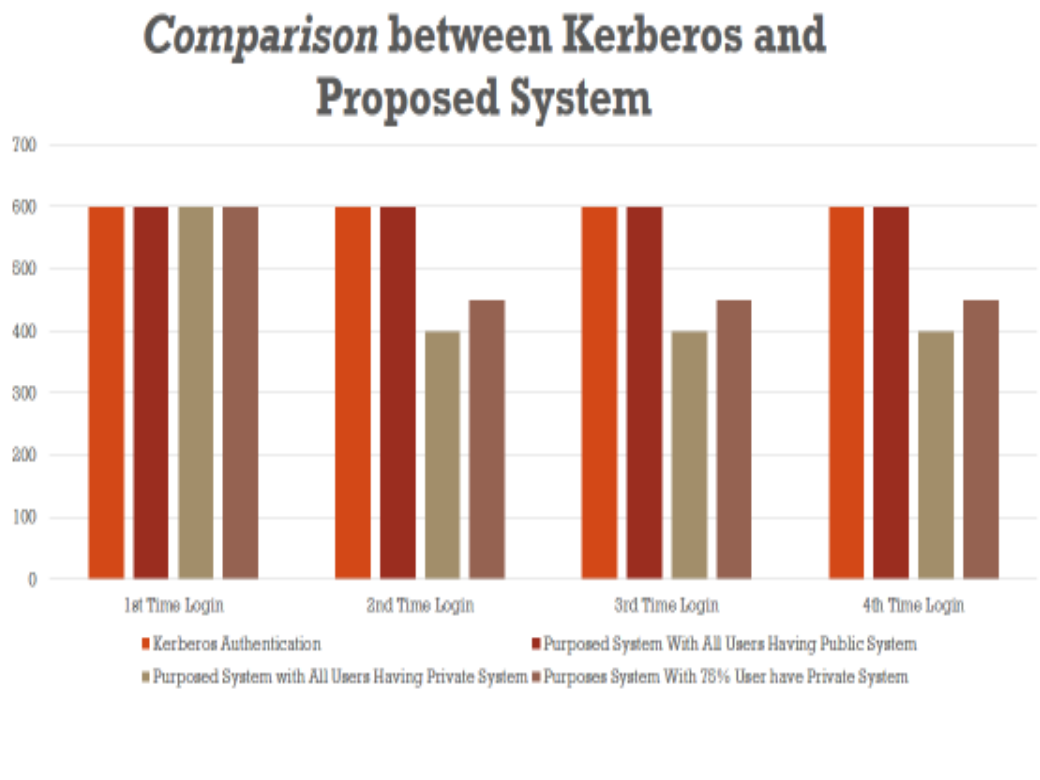

Fig 4.2: Results on Different Systems after successful Logins

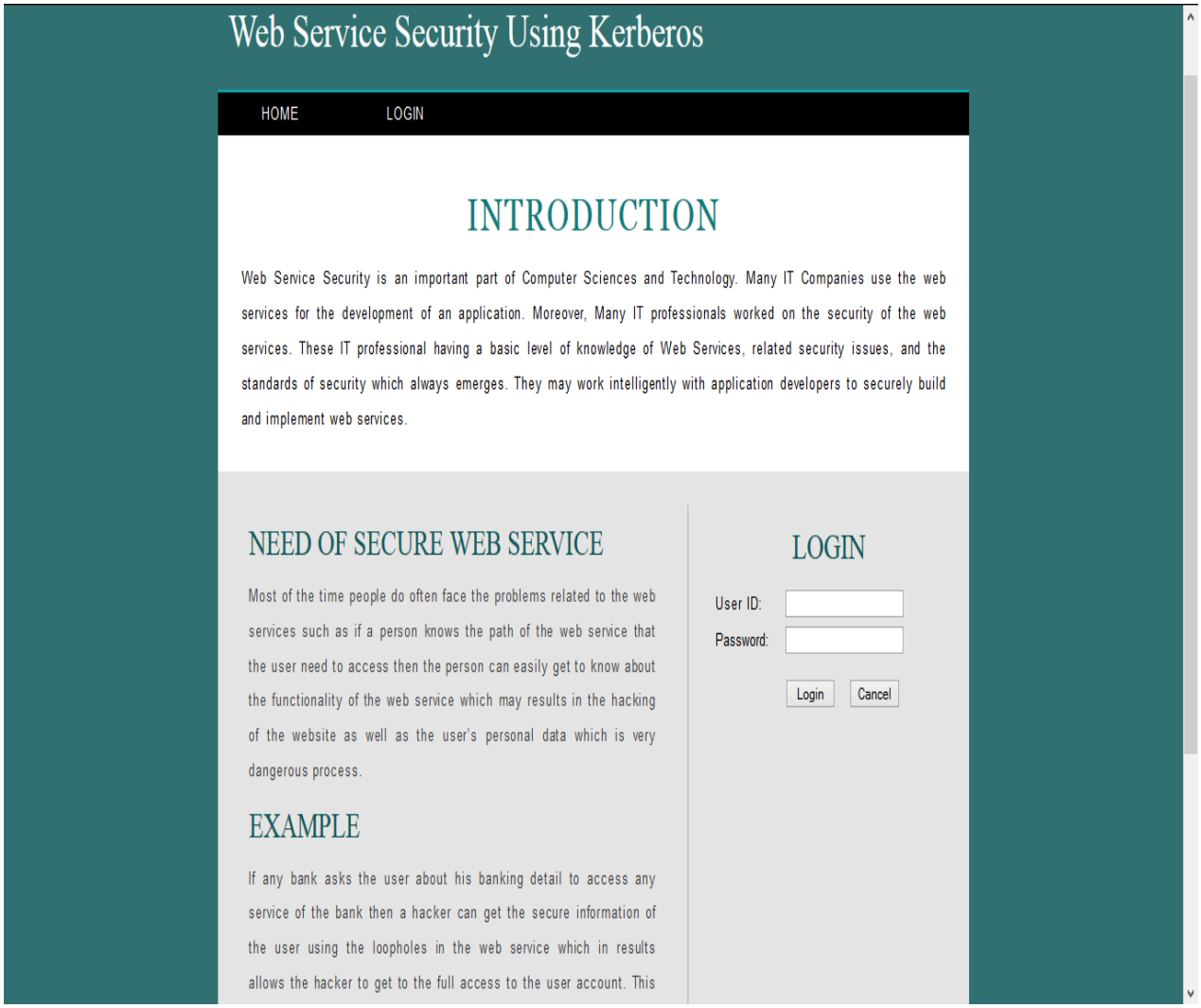

Fig 4.3: Web Service Security Using Kerberos

Figure 4.3 shows the basic introduction of the proposed system along with the login screen for the user of the proposed system. From this home screen the user can easily understand how to use this proposed system and what the benefits of using this proposed system are.

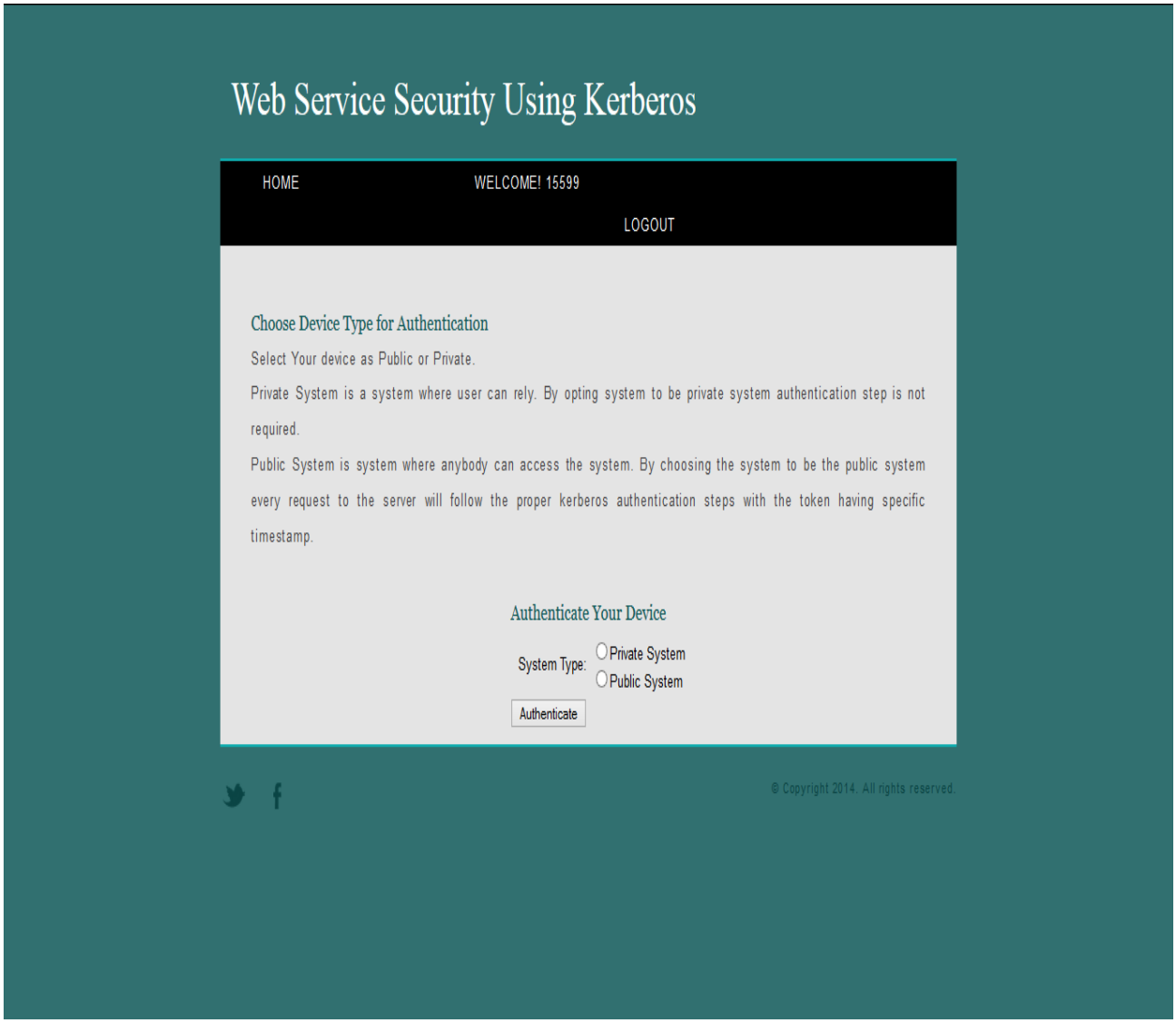

Fig 4.4: Choose Device

Figure 4.4 asks the user to choose the device as a public or private now these two terms are very important for the use of the proposed system. Public systems are specially those system where the access of the system is not limited to one user. Anybody can use this system and can access the resources of the system on the other hand the private system is that system where the access is only limited to one user and other users has the limited access over this system which makes the system to be private and more reliable.

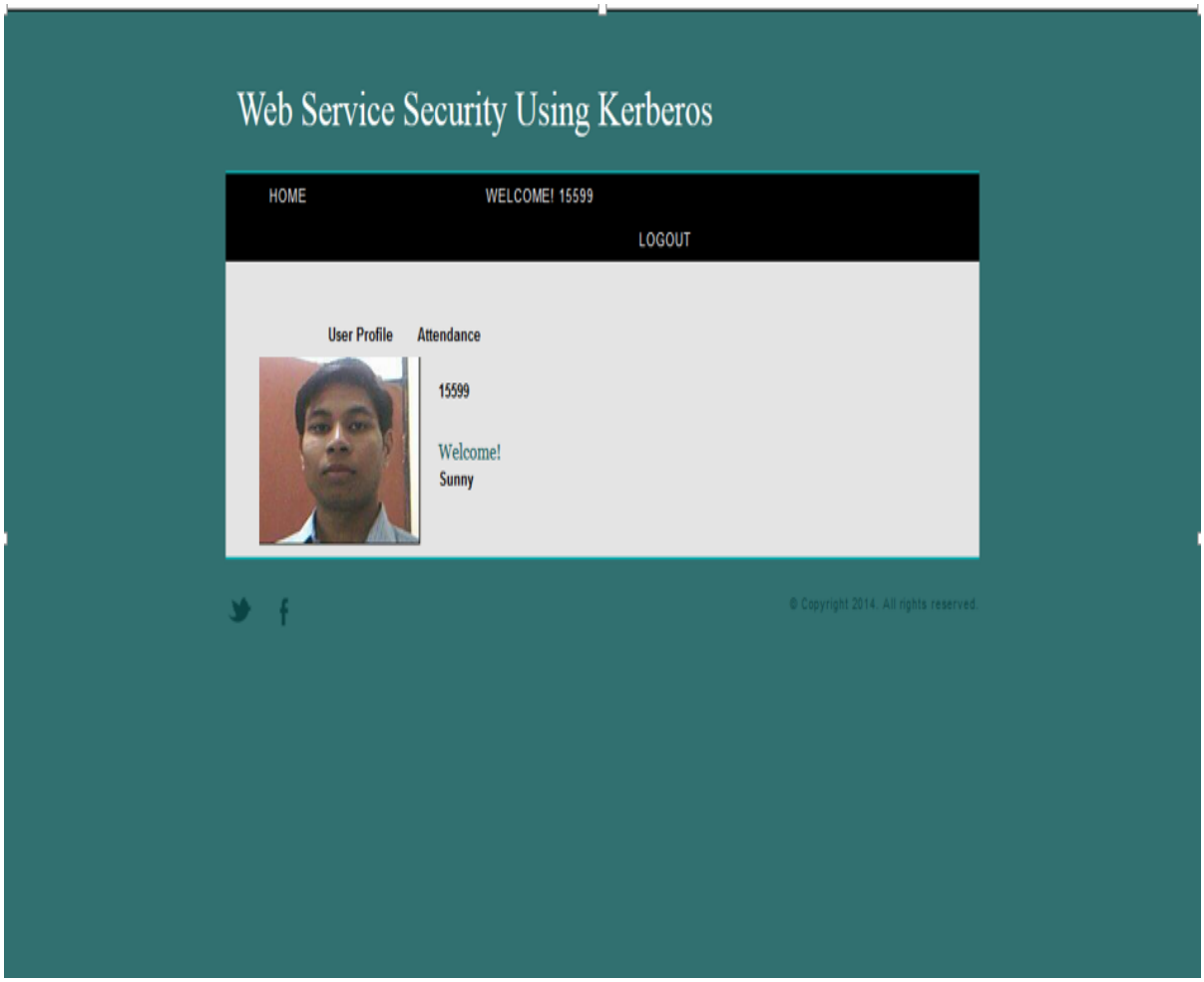

Fig: 4.5 User Home Page

Figure 4.5 illustrates the services the user can access from the proposed system. These services are further divided into staff and the student so that the personal information of the user can be only accessed by the user who is using the proposed system and the services can be only accessed according to the role of the user.

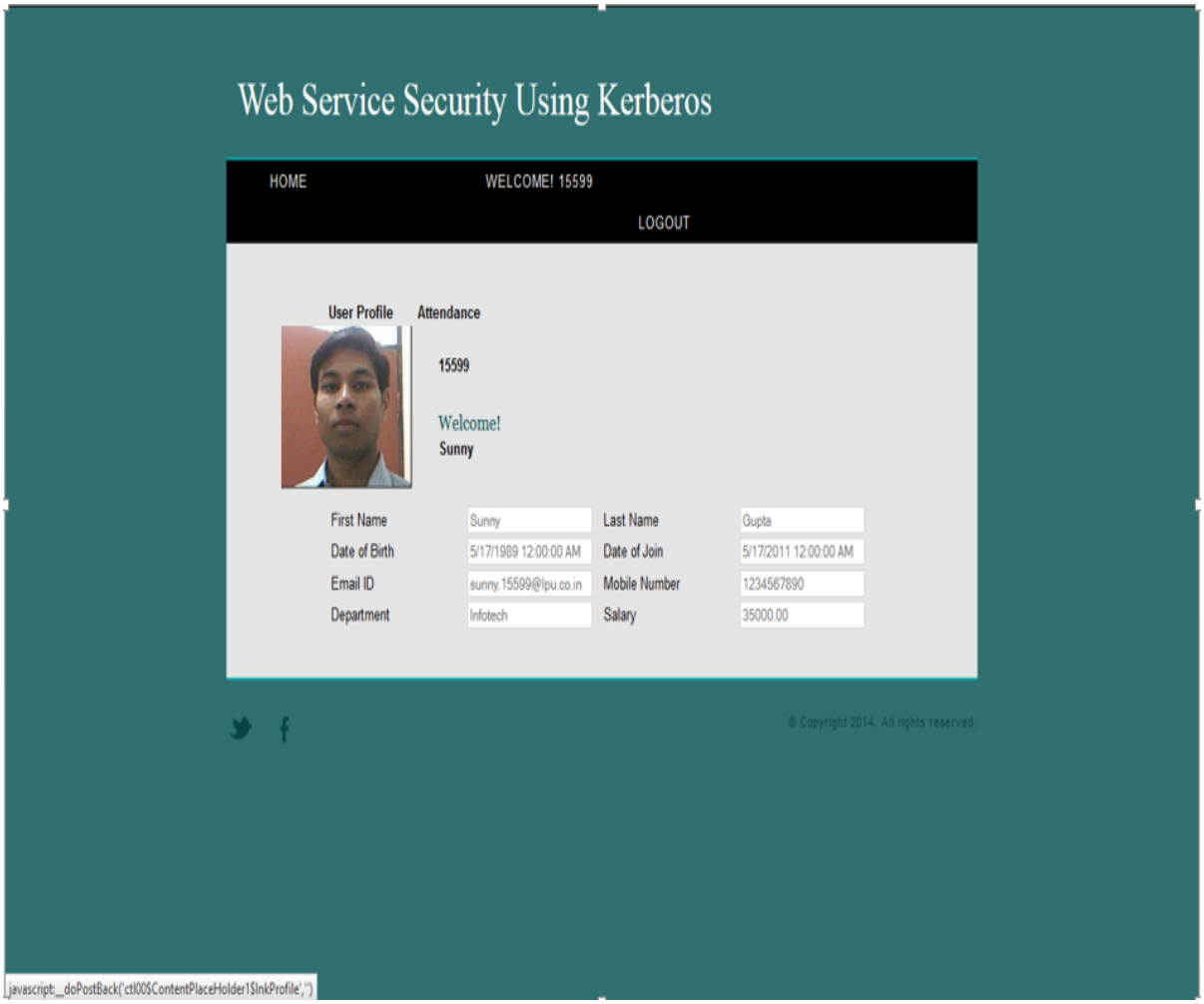

Fig 4.6 User Profile Page

Figure 4.6 shows the service of the employee which is the profile page where the user can see his basic detail in the proposed system.

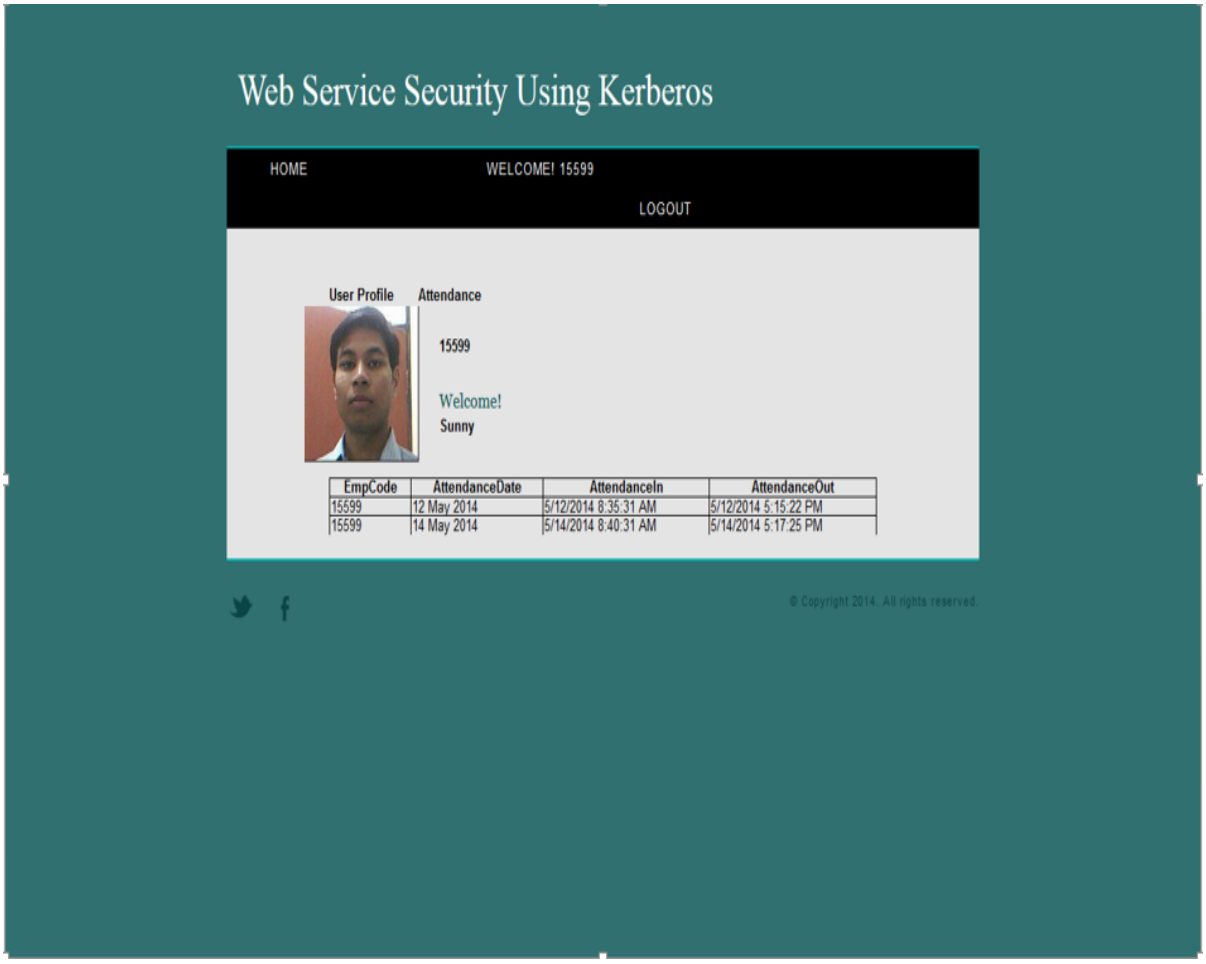

Fig 4.7 Employee Attendance Detail Page

Figure 4.7 shows the service of the employee which is the Employee attendance where the user can see his attendance through the web service in the proposed system.

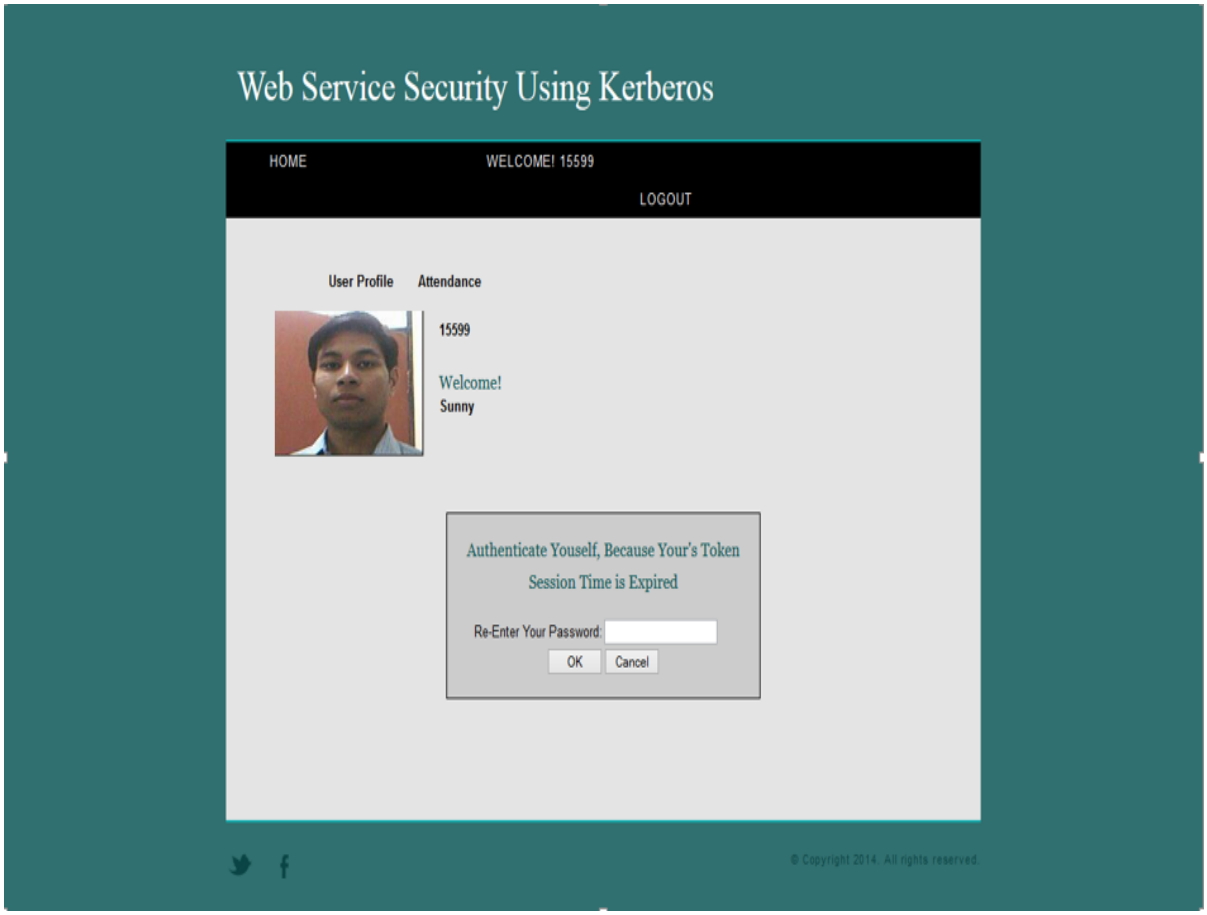

Fig 4.8 System after Token Expire

The figure 4.8 shows the authentication required for the access of the further services from the proposed system which is required only when the user chooses its system to be a public system when the user got successfully authenticated and chooses the device to be a public system then the token has been generated by the system which has the expiry time associated with it. By using this concept the user can access the services of the system until the token got expired after the token expired user need to again enter the authentication detail in order to access the system services.

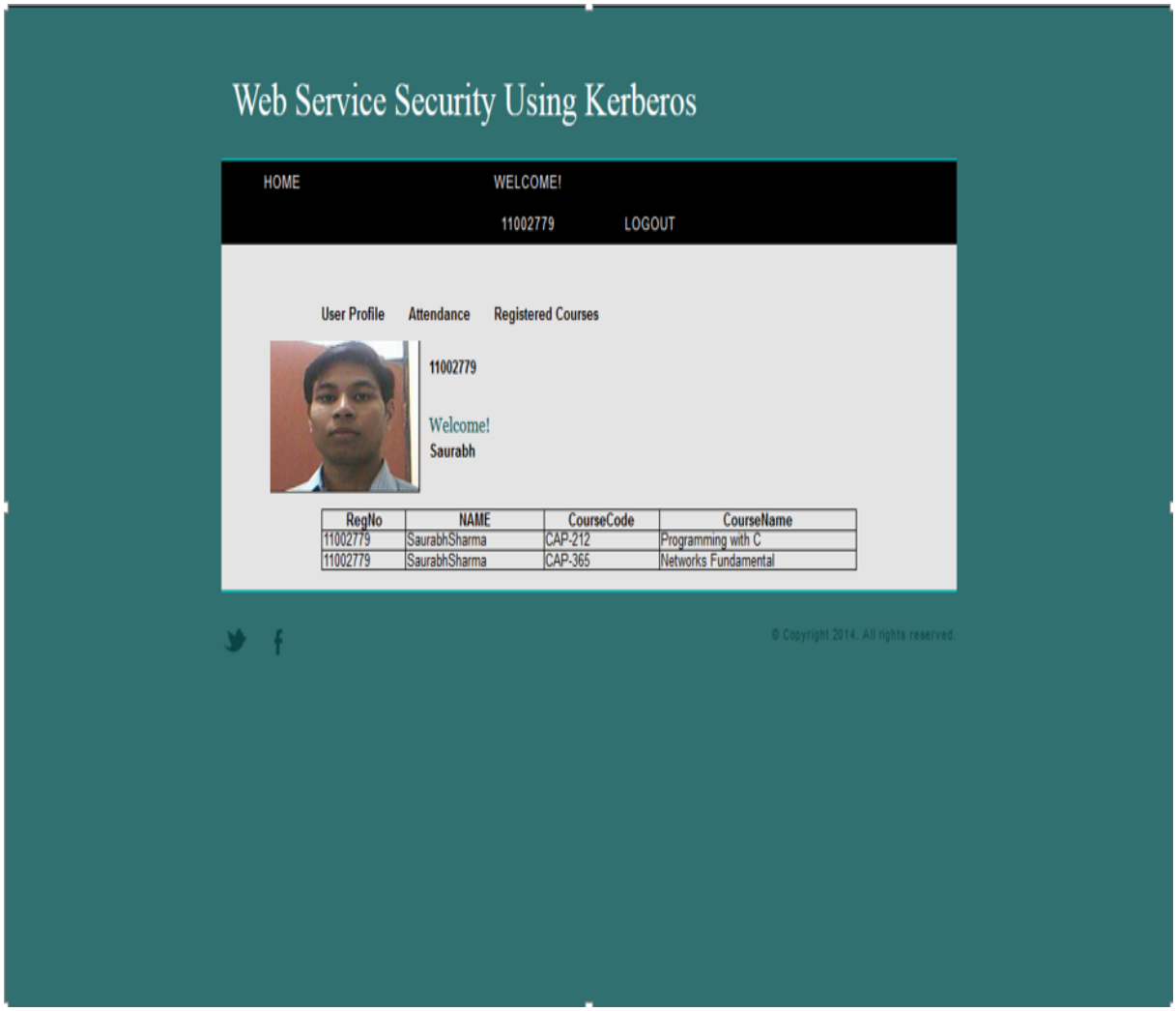

Fig 4.9 Student Course Registration Detail

Figure 4.9 shows the service of the Student in which the student can use the proposed system in order to see the courses in which he is registered and the services of profile and the attendance is also available for the student in the proposed system.

Discussions:

Problem: In order to recognized the system of the user as a private and public system I have used the ip address of the user's system which differentiate the machine of the user for me but later I came to know that the ip address not stay stable these are static for the user who are using the private internet connections or the broadband has the different ip address for every time they logged in to the internet which arises the problem for me to identify the machine of the user who chooses the machine to be a private machine.

Solution: In order to overcome from this problem I uses the mac address instead of the ip address and my problem got solved because the mac address is always unique for the client machine so the client machine can be easily identified as the public or private.

Chapter 5

Conclusion and Future Work

Proposed system requires less number of steps to communicate with server in the process of KDC which leads to time efficient system without missing any security constraint. If the user chooses his/her system as a personal system then our system's improvement is measured by less number of steps in the Communication of the KDC and the server which is done in the step which before the communication of getting session key in KDC and if the user chooses his/her system as public nothing will be changed from previous system as in KDC. The Proposed system allows the user to access or share his/her secure data over the internet with more security and efficiency with the help of secured web service. In future it can be improved for the public system as well as more steps can be reduced from the proposed system which enhance the efficiency of Kerberos without affecting its security policies. With the help of the this secure web services provided by the proposed system the users can use it for the location based services either from their mobile phones or with the help of the tablets. The main advantage of proposed system is that it makes the web services so secure that it guarantees the user that the data which is came to their devices is unchanged which results in providing the correct data to the users and users has the confidence on the information provided by the system. This type of functionality provides the great benefits in the location based services where the users do not want to have any guide with them if they are going to a place which is completely unknown to them. All they have their mobile phones or the devices which uses the location based services which gathered the complete information of the place which the user want to search and act as guide to them so that they reach to a place where they want to go without any difficulty.

The proposed system can be used for the various purpose in the future because nowadays each and everything is now moving towards the use of the web services because web services are the platform independent so that these can be access on either the personal computer or on the mobile devices without any problem. Moreover, the people uses their mobile phones more than their personal computers so the companies are finding the way to provide the universal

application of their product to the users which can be done by the use of the web services. But the only question arises to the companies that how secure their web services are and with what cost. The answer of these both questions is the proposed system which can be easily adapted to any field because of the simple concept and can be easily modified according to the requirement of the product. In future the proposed system can be more refined and can be used in the places like the accessing of the bank services and the e-commerce website or application where the security is prior to any thing.

Chapter 6

References

[1] A. Scedrov, F. Butler, A. D. Jaggard, and C. Walstad (2006) " Formal analysis of Kerberos ," Theoretical Computer Science, vol. 36, no. 1–2, pp. 57–87, Nov. 2006.

[2] Aditya Harbola,Deepti Negi and Deepak Harbola (2012) "A New A3 Kerberos Model", International Journal of Computer Security,2012.

[3] Alin COBÂRZAN(2010) "Consuming Web Services on Mobile Platforms", Conference on Webservice features, 2010.

[4] Amit Kushwaha , Vineet Kushwaha(2011) "Location Based Services using Android Mobile Operating System". IEEE conference on android Development, 2011.

[5] Chi Po Cheong, Chris Chatwin and Rupert Young (2011) "A New Secure Token For Enhancing Web Service Security", International Conference on Web Service Security, 2011.

[6] Emam EL-Emam, Magdy Kutb, Hamdy Kelash and Osama S. Faragallah (2011) "An Authentication Protocol Based on Kerberos 5", International Journal of Computer Application 2011.

[7] H.-Y. Chien and J.-K. Jan (2003) "A hybrid authentication protocol for large Mobile network," The Journal of Systems and Software, vol. 67, no. 2, pp. 123–130, Aug. 2003.

[8] Hao Zeng, Dianfu Ma, Zhuqing Li, Yongwang Zhao(2012) "A Policy-Based Architecture for Web Services Security Processing", Springer 2012 conference on web services.

[9] J.Kohl and C.Neuman(1993) "RFC 1510: The Kerberos Network Authentication Service (V5)," Sep.1993.

[10] Kristin Lauter (2004) "The Advantages of Elliptic Curve Cryptography for wireless Security", Microsoft corporation, IEEE Wireless Communications • February 2004.

[11] Li Jiang, Hao Chen, Fei Deng(2010) "A Security Evaluation Method Based on STRIDE Model for Web Service", IEEE Conference on Web Security, 2010

[12] Manav Singhal, Anupam Shukla(2012) "Implementation of Location based Services in Android using GPS and Web Services", Internation conference on GPS and Location Based Services, 2012.

[13] Mr. S.K. Pathan, Mr. S.N. Deshmukh, Dr. R.R. Deshmukh(2009) "Kerberos Authentication System –A Public Key extension" IEEE 2009, Computer Security

[14] Nikos Mavrogiannopoulos, Andreas Pashalidis and Bart Preneel (2012) "Security implications in Kerberos by the introduction of smart cards", Springer 2012, Security of Computer Application.

[15] R. Sakai, K. Ohgishi, and M. Kasahara(2000) " The 2000 Symposium on Cryptography and Information Security" , . Cryptosystems Based on Pairins, 2000.

[16] Wei Fu, Yingzhou Zhang, Xianting Zhu and Junyan Qian (2012) "WSSecTool: A Web Service Security Analysis Tool Based on Program Slicing", International Conference on Secure Web ,2012.

[17] Xiaohong Li, Yan Caoy, Zhiyong Fengz, RanLiux(2010) "Web Service Security Analysis Model Based on Program Slicing". IJCS on Web service integration and security, 2010.

[18] http://www.giac.org/cissp-papers/47.pdf

[19] http://www.kerberos.org/software/adminkerberos.pdf

[20]http://technet.microsoft.com/en-us/library/cc780469(v=ws.10).aspx

[21]http://searchsecurity.techtarget.com/definition/Kerberos.

[22] http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

Chapter 7

Appendix

7.1 Abbreviations

- **A3 :** Authentication, Authorization and Accounting
- **AS :** Authentication Server
- **FTP :** File Transfer Protocol
- **IP :** Internet Protocol
- **IT :** Information Technology
- **JSON :** JavaScript Object Notation
- **KDC :** Key Distribution Center
- **MDG :** Method Dependence Graph
- **SOAP :** Simple Object Access Protocol
- **TGT :** Ticket Granting Ticket
- **UDDI :** Universal Discovery Description Integration
- **URL :** Universal Resource Locator
- **WSDL :** Web Services Definition Language
- **XML :** Extensible Markup Language

Chapter 8

List of Publications

1. Paper has been published in the **"Wilkes100 -Second International Conference on Computing Sciences"** with title "**Optimization in Kerberos Model".**