ISSN 2395-1621

Numerical Simulation of Gurney Flap On RAE-2822 Airfoil

[#1] Gangaram B. Eakmbe, [#2] Mukesh V. Khot

[1]eakmbeg@gmail.com
[2]mvk234@rediffmail.com

[#12]Department of Mechanical Engineering, TSSM's P.V.P.I.T., Bavdhan, Pune-21, India

ABSTRACT

The fuel economy, High performance and cost effectiveness are the essential parameters in the research and development of aviation industry. With the rise of global demand of commercial aeroplane an increase population it was needed to found out high performance option. The performance and effectiveness of airfoil largely depend on Lift coefficient. The main objective of this study is to increase the aerodynamic performance of aerofoil by increasing the overall Lift to Drag ratio. Previous studies show that Gurney flap (GF) is a simple and effective lift enhancement device, consisting of a small flat tube fitted perpendicular to the pressure surface of aerofoil in the vicinity of trailing edge. After the study it is found that by altering the position, Height, and width of GF with respect to airfoil camber length we can get the optimum value of Lift to drag ratio which is higher than flow over aerofoil with ought GF.

From this study it is found that Lift enhancement is achieved for greater heights of gurney flap but at the expense of increased drag. The rate of lift increment decreases for greater heights and drag increases rapidly for h >2%. So the optimum height of GF is 2% of chord length of airfoil.

ARTICLE INFO

Article History

Received :18th November 2015

Received in revised form :

19th November 2015

Accepted : 21st November , 2015

Published online :

22nd November 2015

Keywords- **Lift coefficient, Drag Coefficient, Gurney Flap, chord length.**

I. INTRODUCTION

The fuel economy, High performance and cost effectiveness are the essential parameters in Aviation industry. Performance as well as other parameters such as take-off and landing distance, payload capacity, Noise produces while take-off and landing, Fuel efficiency and so on, of airfoil depend on Lift to drag ratio. So to improve the performance it is important to improve overall lift to drag ratio. There are plenty of methods available today to enhance the Lift coefficient of airfoil such as making airfoil curved near the trailing edge which turn the flow around the tail and generate the lift, Vertex generation, Oscillating flaps, Hydraulic actuator system, Electromechanical Actuation Systems, By increasing angle of attack and so on [13]. Each method has its own advantages and disadvantages. But it is very important to consider Parameters like effectiveness of system under critical conditions like transonic flow, Production of stole, Operating parameters, Maintenance, Influence to environmental parameters, Mechanical stability and operating and maintenance coast of system while selecting the lift enhancement technique.

The Gurney flap is a flat plate on the order of 1-3% of the airfoil chord in length, oriented perpendicular to the chord line and located on the airfoil windward side at the trailing edge. It was first used by Dan Gurney [13] on the top trailing edge of the rear wing on his race car to provide extra rear end down force with minimal aerodynamics disturbance. Liebeck [13] conducted first wind tunnel experiments on GF. Over the decades, Gurney flap has attracted the attention of engineers and designers by its performance enhancement. A Gurney flap is easy to analyze and manufacture because of its very simple design. As regulations of car races restrict sizes of a vehicle including wing areas, the Gurney flaps are frequently equipped in race cars of Formula One, etc., because of their compactness and lightness, to obtain the high-speed running stability at curves. In the case of road vehicles, shape optimization and equipment of aerodynamic devices such as wings enhances the down force, i.e. negative lift, and consequently does the friction force of tires against the road. The down force can be furthermore increased by adding high-lift devices to wings, as the lift force in the case of airplanes. The same

principle is applied in a reverse manner to airfoil, i.e. to increase the lift force.

The flow over an airfoil with gurney flap is shown in figure 01 below, due to small flap at trailing edge the lower stream flow delayed to reach the trailing edge creating the counter-clockwise vertex in front of flap that causes upper stream flow to flows continuously as shown in fig. Two contra dictionary vertices create lower pressure region behind the flap at trailing edge. That prevents the boundary layer separation. That enhances the lift at trailing edge. This is proved by using Helmholtz theorem about vorticity by this theory lift is directly proportional to the circulation.

i.e $\frac{L}{b} = \rho \times V_0 \times \Gamma$

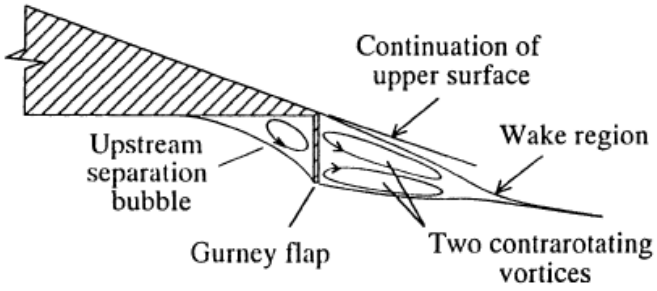

Fig. 01: Hypothesized trailing edge flow structure for an airfoil with a Gurney flap [04]

RAE 2822 airfoil has been experimentally tested under the flow conditions that generate a transonic, turbulent and a shock induced separated flow environment. This airfoil is the best suitable one for so many applications and gives the optimal solutions in the particular cases which cannot be able obtain by using the other airfoils. The RAE stands for **Research Assessment Exercise** was an exercise undertaken approximately every 5 years on behalf of the four UK higher education funding councils i.e. Higher Education Funding Council for England (HEFCE), the Scottish Funding Council (SFC), the Higher Education Funding Council for Wales (HEFCW) and the Department for Employment and Learning, Northern Ireland (DEL) to evaluate the quality of research undertaken by British higher education institutions [9]. The RAE provides quality ratings for research across all disciplines.

RAE 2822 airfoil has been experimentally tested under the flow conditions that generate a transonic, turbulent and a shock induced separated flow environment. This airfoil is the best suitable one for so many applications and gives the optimal solutions in the particular cases which cannot be able obtain by using the other airfoils.

Shubham Jain, N. Sitaram, Sriram Krishnaswamy [6], performed computational investigations on the aerodynamics effects of gurney flap on Airfoil NACA 0012 is examined. This computational study comprises of steady state, 2-D model and uses k-ε RNG turbulence model of FLUENT. Airfoil with GF is analyzed for six different heights from 0.5% to 4% of the chord length, seven positions from 0% to 20% of the chord length from the trailing edge and seven mounting angles from 30^0 to 120^0 with the chord. Computed values of lift and drag coefficients with angle of attack are compared with experimental values and good agreement found at low angles of attack.

I. GEOMETRY MODELLING AND GRID GENERATION

The slandered shape of RAE2822 is shown in following fig.

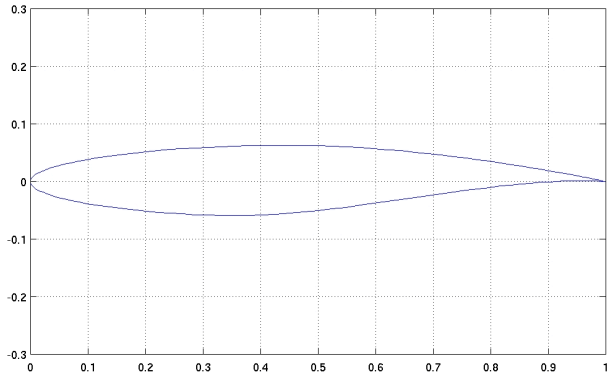

Fig. 2: RAE2822 airfoil [11].

In RAE2822 first number is maximum camber in percentage of chord (airfoil length). Second number is location of maximum camber in tenths of chord measured from LE. Last two digits give maximum thickness (t) in percentage of chord. The Gurney flap is attached at trailing edge of length in percentage of chord length using pre-processing tool ANSA1500.

The computational domain designed in a such a way that the Upper and lower boundaries of the simulation domain are 10 chord lengths away from the airfoil chord, which is defined as the velocity-inlet boundary condition, and the downstream outflow boundary is 20 chord lengths away. The surface boundaries of the airfoil and the GF are set as a no-slip wall condition. The C- grid mesh is generated with the help of STAR-CCM+ 9.02.

The 16 boundary layers are generated around the airfoil so that the flow near the boundary of airfoil will resolve properly. The first grid point above the surface, which locates at *y*+ approximately equal to one is 5×10^-6 times of chord length away. The other boundary layers are generated with expansion ratio of 1.1. The mesh in the area of shock wave are made fine and in other places gradually increased so that the total cell count would be optimum and time required to run the simulation is less.

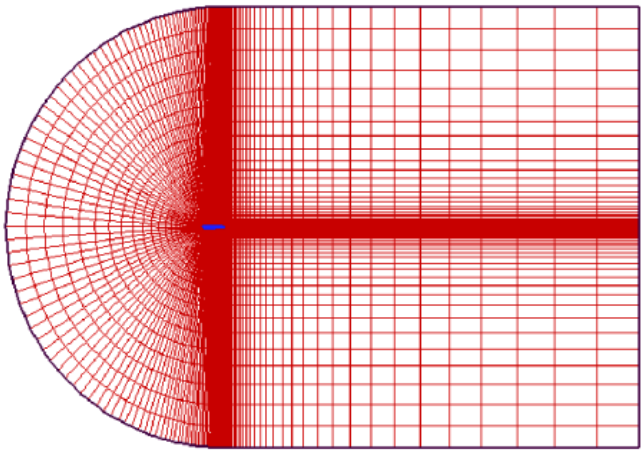

Fig. 3: C- grid mesh around RAE2822 airfoil with GF.

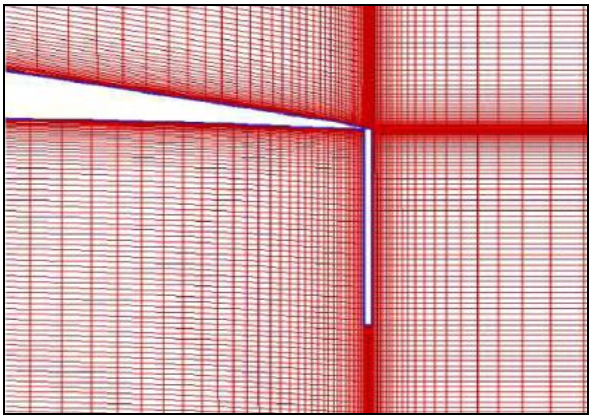

Fig. 4: C- Zoom view of mesh around GF.

II. BOUNDARY CONDITIONS AND SOLVER SETTINGS.

The airfoil boundary is assigned as solid-wall with no-slip condition while inlet is assigned as velocity inlet and outlet is assigned as pressure-outlet conditions. Free stream velocity is 85 m/s, and the Reynolds number based on chord length is *Re* = 5.*8* ×10^6. The Mach number used is 0.725 and The fluid properties used are density of 1.225 kg/m3 and viscosity of 1.795×10^-5 (kg/ms).

In this example, the flow is steady, turbulent and compressible. The default Spalart-Allmaras turbulence model and the ideal gas model will be used. The analysis will also use the coupled solver, which is recommended for all supersonic and transonic compressible flows.

III. RESULTS AND DISCUSSION.

To validate the result of flow over an airfoil RAE2822 with GF, The numerical simulation of airfoil RAE2822 withaught GF is performed and compared with the experimental results from reference [4], the experimental results available are for Mach number below 0.3 i.e. subsonic flow but the comparison shows that the result obtained by numerical solution are linear with the experimental result.

The graph of variation of lift coefficient against the increase of Angle of attack is plotted with varying height of Gurney flap. The lift coefficient value of airfoil RAE2822 is obtained at gurney flap height of 0.5% to 3% chord length and angle of attack from 0 to 15 degree.

Similarly value of drag coefficient are also obtained and plotted against the angle of attack for Gurney flap height of 0.5% to 3% chord length.

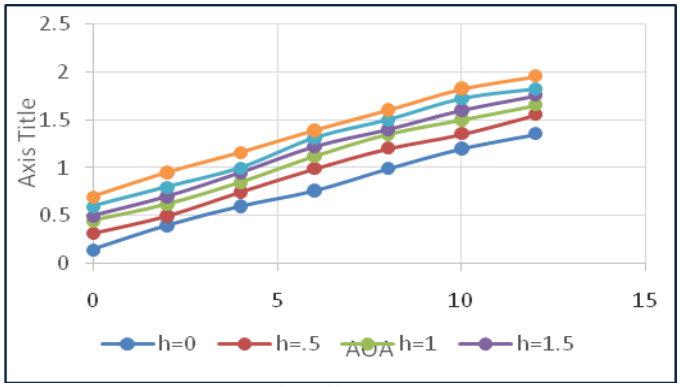

Fig. 05: Lift coefficient v/s AOA

From the data obtained and data available we can say that increase in Lift coefficient for 0.5%, 1%, 1.5%, 2%, 3% flap height is 25%, 36%, 47%, 53%, 67% respectively. Apart from increasing the C_L values at a given incidence, maximum C_L Values compared with clean airfoil are also increased by 19%, 23%, 31%, 36%, 42% when flap heights of 0.5%, 1%, 1.5%, 2%, 3% are used respectively. The increment in maximum CL decreases as the flap height increases.

IV. CONCLUSION AND FUTURE STUDY.

A numerical simulation was performed to examine the aerodynamic performance of the RAE-2822 S-C airfoil induced by a GF with different heights at subsonic and transonic speeds. The following conclusions could be made:

Lift enhancement is achieved for greater heights but at the expense of increased drag. The rate of lift increment decreases for greater heights and drag increases rapidly for h >2%.The GF can be used effectively up to height of 2% of chord length but more than that it produce adverse effect in the form of drag force. The optimum GF position and angle at the trailing edge of airfoil would also help to improvise result, as well as the drag reduction techniques can also be applied at the leading edge of airfoil with GF at trailing edge.

REFERENCES

[1] https://Nptl.ac.in/Airodynamics/Airfoils/and/Wings .pdf

[2] Masan W.H. *Configuration Aerodynamics*, Virginia Tech. Blacksburg, VA. Jan 2006. pp 7-1, 7-35.

[3] Bernardus Maria Spee, 6Investigations On The Transonic Flow Around Aerofoils, *National Aerospace Laboratory*, pp 5,11,23

[4] Roy Animesh, Low speed wind tunnel test of a 300 sweptback wing at different manual condition,*A thisis submitted to Jodhavpur university may2013*.pp 05-09

[5] Witteveen, J. A. S., Doostan A., Iaccarino G "Uncertainty quantification of the transonic flow around the RAE 2822 airfoil" *Center for Turbulence Research, 2009*. pp 3,9,10, 38

[6] Shubham Jain1 N. Sitaram2 Sriram Krishnaswamy Computational Investigations on the Effects of Gurney Flap on Airfoil Aerodynamics *Journal of Aircraft (0021-8669)*. pp 11,25-28.

[7] Eric Fred Davis, A Study Of Gurney Flaps And Their Influence On An Airfoil In Ground Effect, *Oklahoma State University, Dec, 2010.* p.p 13,17

[8] Cory S. Jang, James C. Ross, Russell M. Cummings, Numerical investigation of an airfoil with a Gurney flap, *NASA Ames Research Center, Moffett Field, CA 94035, USA.* p.p 08

[9] Giguere, P.; Lemay, J.; Dumas, G. (1995). "Gurney flap effects and scaling for low-speed airfoils". "AIAA Applied Aerodynamics Conference, 13 th, San Diego, CA, Technical Papers. Pt. 2". pp. 10,13.

[10] www.airfoilstools.com/airfoiltools/search/NACA/index

[11] Catalano, F. M. Experimental And Numerical Study Of A Two element Wing With Gurney Flap *25th*

International Congress Of The Aeronautical Sciences, 2006.

[12] Y. Takakura, T. Kobayash, M. Takag, Visualization Of Flow Fields About An Airfoil With A Gurney Flap *15th International Symposium on Flow Visualization, June 25-28, 2012, Minsk, Belarus.*

[13] Myose, R.; Papadakis, M.; Heron, I. (2009). "Gurney flap experiments on airfoils, wings, and reflection plane model".*Journal of Aircraft 35.* pp 11,14.

[14] https://sites.google.com/site/danhirschfeld2/The/story/on/the/urney/flap.html.

Web delivered services and applications have increased in both popularity and complexity over the past few years. Daily tasks, such as banking, travel, and social networking, are all done via the web. Such services typically employ a web server front end that runs the application user interface logic, as well as a back-end server that consists of a database or file server. Due to their ubiquitous use for personal and/or corporate data, web services have always been the target of attacks. These attacks have recently become more diverse, as attention has shifted from attacking the front end to exploiting vulnerabilities of the web applications in order to corrupt the back-end database system (e.g., SQL injection attacks).

A plethora of Intrusion Detection Systems (IDSs) currently examine network packets individually within both the web server and the database system. However, there is very little work being performed on multitier Anomaly Detection (AD) systems that generate models of network behavior for both web and database network interactions. In such multitier architectures, the back-end database server is often protected behind a firewall while the web servers are remotely accessible over the Internet. Unfortunately, though they are protected from direct remote attacks, the back-end systems are susceptible to attacks that use web requests as a means to exploit the back end.

To protect multitier web services, Intrusion detection systems have been widely used to detect known attacks by matching misused traffic patterns or signatures. A class of IDS that leverages machine learning can also detect unknown attacks by identifying abnormal net-work traffic that deviates from the so-called "normal" behavior previously profiled during the IDS training phase. Individually, the web IDS and the database IDS can detect abnormal network traffic sent to either of them. However, we found that these IDSs cannot detect cases wherein normal traffic is used to attack the web server and the database server.

For example, if an attacker with non admin privileges can log in to a web server using normal-user access credentials, he/she can find a way to issue a privileged database query by exploiting vulnerabilities in the web server. Neither the web IDS nor the database IDS would detect this type of attack since the web IDS would merely see typical user login traffic and the database IDS would see only the normal traffic of a privileged user. This type of attack can be readily detected if the database IDS can identify that a privileged request from the web server is not associated with user-privileged access. Unfortunately, within the current multithreaded web server architecture, it is not feasible to detect or profile such causal mapping between web server traffic and DB server traffic since traffic cannot be clearly attributed to user sessions.

We present Double Guard, a system used to detect attacks in multitier web services. Our approach can create normality models of isolated user sessions that include both the web front-end (HTTP) and back-end (File or SQL) network transactions. To achieve this, we employ a light-weight virtualization technique to assign each user's web session to dedicated container, an isolated virtual computing environment. We use the container ID to accurately associate the web request with the subsequent DB queries. Thus, Double Guard can build a causal mapping profile by taking both the web server and DB traffic into account.

II. RELATED WORK

Double guard and its classification:-

Double Guard is a system used to detect attacks in multitier web services [1] [2].A network Intrusion Detection System can be classified into two types: anomaly detection and misuse detection. Anomaly detection first requires the IDS to define
and characterize the correct and acceptable static form and dynamic behaviour of the system, which can then be used to detect abnormal changes or anomalous behaviours. The boundary between acceptable and anomalous forms of stored code and data is precisely definable. Behaviour models are built by performing a statistical analysis on historical data or by using rule-based approaches to specify behaviour patterns. An anomaly detector then compares actual usage patterns against established models to identify abnormal events [1] [2] [3].

Methodology:-

This approach can create normality models of isolated user sessions that include both the web front-end (HTTP) and back-end (File or SQL) network transactions [1] [3]. It employs a light-weight virtualization technique [1] [3] to assign each users web session to a dedicated container, an isolated virtual computing environment. It uses the

container ID to accurately associate the web request with the subsequent
DB queries. Double Guard forms container-based IDS with multiple input streams to produce alerts. The correlation of input streams provides a better characterization of the system for anomaly detection because the intrusion sensor has a more precise normality model that detects a wider range of threats[1] [2] [3] [4].

Possible Attacks:-

Some of the important attacks are generally used by attackers for hacking i.e. SQL injection, Direct DB Attack ,Hijack future session attack, Privilege escalation[1] [2] [3] [5]and D-DOS attack [1].

Algorithm Used:-

In order to detect such attacks algorithms which are being used are Static model building algorithm [1] [2] [3] [4].

Limitations:-

Vulnerabilities Due to Improper Input Processing :-

Once the malicious user inputs are normalized, Double Guard cannot detect attacks hidden in the values [1].

Possibility Of Evading Double Guard :-

It is possible for an attacker to discover the mapping patterns by doing code analysis or reverse engineering, and issue expected web requests prior to performing malicious database queries [1].

Distributed DOS attacks:-

Previous Double Guard system was not designed to mitigate D-DOS attacks. These attacks can also occur in the server architecture without the back-end database. Denial-of-service attacks are common and fashionable these days. In denial-of service attack, attacker tries to prevent legitimate users from using a service or shutting down a service owing to some implementation vulnerability crashing the machine [1].

III.DOUBLE GUARD SYSTEM ARCHITECTURE

System architecture:-

This is the system architecture design. In this, first the client sends a request for price and other information related to a particular product then that request is analyzed in order to identify if the request is HTTP request or a query and this is done using static model building algorithm.

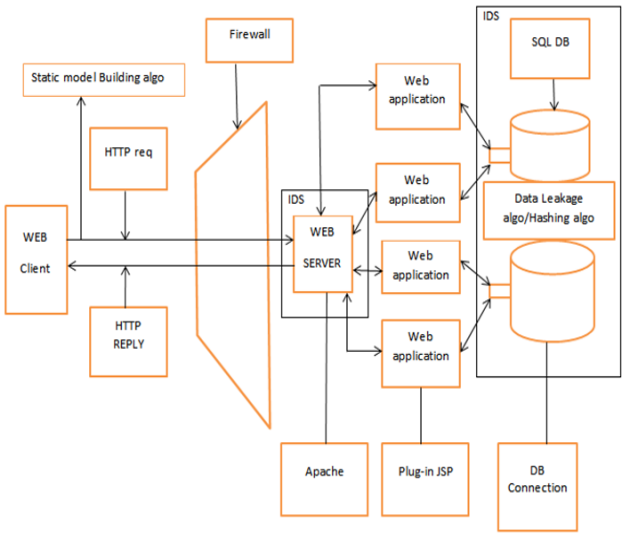

Figure 3.1: System Architecture diagram

After the request is categorized if the request is HTTP request then that request is passed through firewall and web server receives that request and that request is send as a query to database server and response is sent accordingly but the request is handled only after user authentication is satisfied .If the values in database is changed then data leakage occurs and that's when data leakage algorithm works and saves the
records of unauthorized user and sends it to admin. If a particular authorized user requests for hacked data then previous data is provided to that user and this is done using hashing algorithm.

Attacks scenario:-

1. ***SQL-Injection Attacks:-***

Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the data or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database [fig 2]. Since our approach provides a two-tier detection, even if the exploits are accepted by the web server, the relayed contents to the DB server would not be able to take on the expected structure for the given web server request.

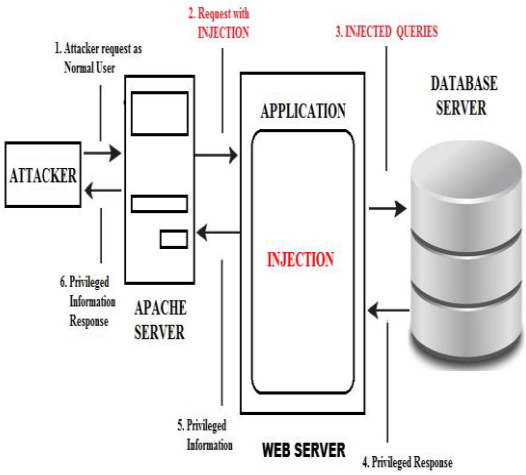

Fig 3.2 SQL- injection attack [5]

Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the data or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database. Since our approach provides two-tier detection, even if the exploits are accepted by the web server, the relayed contents to the DB server would not be able to take on the expected structure for the given web server request. For instance, since the SQL injection attack changes the structure of the SQL queries even if the injected data were to go through the web server side, it would generate SQL queries in a different structure that could be detected as a deviation from the SQL query structure that would normally follow such a web request.

2. D-Dos Attacks:-

Double Guard is not designed to mitigate D-DoS attacks [fig 3]. These attacks can also occur in the server architecture without the backend database. In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. A distributed denial-of-service (D-DoS) is where the attack source is more than one–and often thousands–of unique IP addresses. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web server such as banks, credit card payment gateways; but motives of revenge, blackmail or activism can be behind other attacks. A distributed denial-of-service (D-DoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems flooding the targeted system with traffic.

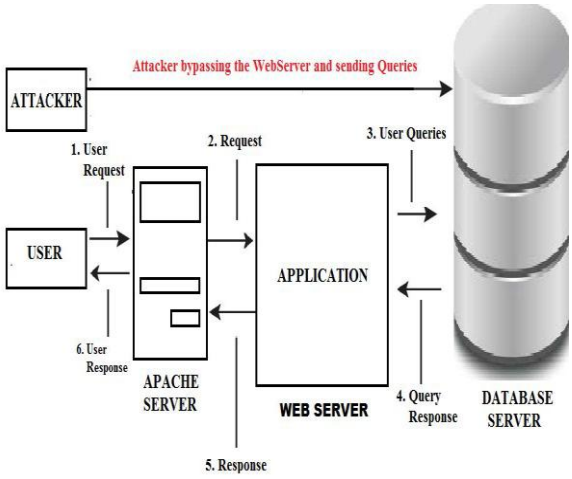

Fig 3.3 D-DoS attack

When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time. Malware can carry D-DoS attack mechanisms; one of the better-known examples of this was My Doom. Its DoS mechanism was triggered on a specific date and time. This type of D-DoS involved hard coding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

IV.ALGORITHM

Static Model Building Algorithm (I):-

Ensure: The Mapping Model for static website

Input: Set AQ for database query. Set AR for server request.

Step 1: Identify the input type of HTTP request whether it is a query or a request.

Step 2: for each different request do, if r is a request to static file.

Step 3: Store the input in hash table as per their type AQ for query and for request AR.

Step 4: The key for hash table entry will be set as the input itself.

Step 5: Forward AQ and AR to virtual server to validate.

Step 6: If attack identified then virtual system automatically terminate the HTTP request.

Step 7: Else HTTP request is forwarded to the original server.

Step 8: Display information.

Step 9: Exit.

Data leakage algorithm (II):-

Input: Input data D = D1, D2, D3,.., Dn saves into the hash table.
Step 1: Arrange all input data into matrix format (save into log files).
Step 2: Consider m as a selected data act as a new selected data.
Step 3: m position gets changed after allocated time period.
Step 4: If Ms data get hacked.
Step 5: Data leakage is occurs.
Step 6: We have to check the leakage data and prevent
Step 7: Using Revert back function we have to get original data.
Step 8: When user calls that corrupted file, hash function gives to user a previous data.
Step 9: Return True.

MD5 Hashing algorithm (III):-

MD5 which stands for Message Digest algorithm 5 is a widely used cryptographic hash function The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size hash value as the output The input data can be of any size or length, but the output hash value size is always fixed

Step 1: Start

Step 2: For each candidate set element.

Step 3: For PV (i) and CV (i) compare attributes and detect which fields are corrupted.

Step 4: get who and when of corruption event.

Step 5: Prepare a report.

Step 6: Stop

V.FUTURE SCOPE

The basic idea is provide two tier security to for web applications. The aim is to secure the web server from the attacker client and to secure the data from the internal authorized persons in the data care centres. This security model can be further extended to provide security against other attacks.

VII.CONCLUSION

This paper States the design level approach taken by team for the project. In this document, a fair amount of elaboration has been done on the project scenario pointing out the most of the important detail. The goal for the final product has become
apparent as the scenario and the desired user interface is visually explained. Additionally, this report defines proposed system architecture and is discussed with attacks scenario. Further information on the technical design is given and progress is summarized. In this the system architecture is designed for detecting intrusions like SQL injection and D-Dos attacks.

REFERENCE

[1].Mixing Le, Angelos Stavros, Member, IEEE, and Brent ByungHoon Kang, Member, IEEE, IEEE Transactions on dependable and secure computing, Double Guard: Detecting Intrusions in Multitier Web Applications, VOL. 9,NO. 4, March, 2014.
[2]. Mr. Chaudhari Hitesh Kumar, Prof. Ajay V. Nadargi, Mr. Bodade Narendra, Mr. Shinde Sushil , Double Guard: Detecting Intrusions in Multi-tier Web applications, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015.
[3].K.Karthika, K.Sripriyadevi, To Detect Intrusions in Multitier Web Applications by using Double Guard Approach., International Journal of Scientific and Engineering Research Volume 4, Issue 1, January-2013.
[4]. ShapnaRani.E, G.Sathesh Kumar, Mythili.R, Karthick.R. Intrusion Detection System for Multitier Web Applications Using Double Guard, International Journal of Engineering And Computer Science ISSN: 2319-7242 Volume 2 Issue 7 (July 2013), Page No. 2162-2166.
[5].Niraj Gaikwad, Swapnil Kandage, Dhanashri Gholap, Double Guard: Detecting and Preventing Intrusions in Multitier Web Applications, Networks and Systems, 2(2), February March 2013, International Journal of Networks and system.

