**INTRUSION DETECTION AND PREVENTION SYSTEM AGAINST dns, xss and cookie poisoning**

**DOMAIN INTRODUCTION:**

**Information Security:**

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

**IT security**

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.

**Information assurance**

The act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

**Threats**

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect you from some of these attacks but one of the most functional precautions is user carefulness.

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. A key concern for organizations is the derivation of the optimal amount to invest, from an economics perspective, on information security. The Gordon-Loeb Model provides a mathematical economic approach for addressing this latter concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics.

**OBJECTIVE:**

The objective of this project is to develop a secure intrusion detection and prevention architecture against 3 vulnerable server cloud attacks.

**PROBLEM STATEMENT:**

Cloud Computing is not necessarily more or less secure than the current environment although it does create new risks, new threats, new challenges and new opportunities as with any new technology. In some cases moving to the cloud provides an opportunity to re-architect older applications and infrastructure to meet or exceed modern security requirements. Cloud computing, security concerns have led organizations to hesitate to move critical resources to the cloud.

**INTRODUCTION:**

Web application ﬁrewalls (WAFs) protect enterprise web systems from malicious attacks. As a facade to the web application they protect, WAFs inspect incoming HTTP messages and decide whether blocking or forwarding them to the target web application. The decision is often performed based on asset of rules, which a redesigned to detect attack patterns. Since cyber-attacks are increasingly sophisticated, WAF rules tend to become complex and difﬁcult to manually maintain and test. Therefore, automated testing techniques for WAFs are crucial to prevent malicious requests from reaching web applications and services.

Threats and risk conditions should be broke down for advanced security and is instrumental while selecting and deploying appropriate security controls ideally. High risk factors or threats to the cloud computing environment incorporate Insecure Application Programming Interfaces, Malicious Insiders, Shared Technology Vulnerabilities, Data Loss/Leakage and Account Service and Traffic Hijacking.

DNS servers are also classified into two types. One is to directly flood DNS servers by sending a large number of DNS requests or other useless traffic.

Since the DNS servers cannot easily distinguish the legitimate requests from the attack traffic, they would simply accept both of them and send the responses. The effective and deployable defense against this attack is to over-provision the network capacity and numbers of servers. The other attack strategy is to exploit DNS servers to amplify attack traffic. The attacker crafts a DNS request that gets a response significantly larger than the request itself, e.g., a 50byterequest for a 500-byte response. The amplified response is replied to a spoofed third-party victim machine. Under this attack, both the amplifying DNS server’s upstream bandwidth and the third-party machine’s downstream bandwidth could be exhausted. Due to traffic amplification, an attacker can exhaust the bandwidth of its victims even if his bandwidth is 10 times smaller. An effective defense against spoofing-based DoS attacks on DNS servers requires source address spoof detection. Assuming a DNS server can distinguish between spoofed requests from real ones, it can selectively drop those spoofed ones with little collateral damage.

DNS allows users to locate resources on the network by converting friendly, human-readable names like www.microsoft.com to IP addresses that computers can connect to. An often-used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.xyz.com translates to the addresses 20.52.88.12 (IPv4).

XSS is a method used to steal data from users by infecting the web pages with malicious scripts (VBScript, JavaScript, ActiveX, Flash) in order to collect sensitive content from the victim. XSS is aiming the dynamic web pages that are interpreted by the web-browsers, so the malicious scripts will be executed locally on the user’s machine and

sensitive data gathered in this way will be transferred from the victim’s computer to the attacker’s location. Usually, attackers spread malicious links over the internet, waiting for the users to click.

Cookie poisoning is the modification of a cookie (personal information in a Web user's computer) by an attacker to gain unauthorized information about the user for purposes such as identity theft. Cookies stored on your computer's hard drive maintain bits of information that allow Web sites you visit to authenticate your identity, speed up your transactions, monitor your behavior, and personalize their presentations for you. However, cookies can also be accessed by persons unauthorized to do so. Unless security measures are in place, an attacker can examine a cookie to determine its purpose and edit it so that it helps them get user information from the Web site that sent the cookie.

**BENEFITS:**

1. Automatic security rendering against 3 cloud attacks using machine learning based intrusion prevention approach.
2. Manual approach and error can be eliminated.
3. Providing secure web application against intrusions.

**CHALLENGES:**

1. We are restricted to perform the attacks in local servers as in real servers we cannot perform the attacking scripts or malicious scripts.

**ABSTRACT:**

Web application ﬁrewalls (WAFs) are an essential protection mechanism for online software systems. Because of the relentless ﬂow of new kinds of attacks as well as their increased sophistication, WAFs have to be updated and tested regularly to prevent attackers from easily circumventing them.

Cloud Computing do not keep data on the user’s system, so there is a need of data security. In our proposed system we focus on recent cloud attacks such as **Cross Site Scripting (XSS) attacks, Domain-Name-Server (DNS) server attacks** and **Cookie poisoning attacks.** We propose **fuzzy** based intrusion prevention techniques. In which we have the advantage of automatic intrusion prevention system by having a trained dataset of previous attack patterns.

The intrusion prevention technique for XSS and Cookie poisoning is been performed using domain name validation and data encryption using advanced encryption standard.The intrusion prevention technique for DNS is been performed using validating and checking the unwanted external / internal links using link guard, eliminating malicious IP address & automatically block the IP and check for any malicious requests.