SAFELI[8], a static analysis framework for identifying SQLi vulnerabilities, inspects the byte code of an ASP.NET application using symbolic execution. The attack patterns are stored in an attack library for pattern matching and a hybrid constraint solver is employed to find the malicious query for each hotspot and then error trace it step by step. The drawback is that this system functions only on ASP.NET based web applications and also can prevent only SQLi attacks.

A Web Application Based Intrusion Detection Framework (WAIDS)[9] proposes a profile matching based approach for the web request data. Keyword extraction and similarity measure for detecting malicious activity are the main techniques employed in this tool. This tool however requires extensive developer knowledge and is complex to implement.

A Web Application Firewall (WAF)[10] is an appliance, server plugin or filter that applies to a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules according to the application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified. This system functions by filtering the data packets at the network layer.

Intrusion Detection Systems (IDS) and Intrusion Detection and Prevention Systems (IDPS) are available from third party vendors. However, these systems are costly and also function only on the network layer.

Other proposed systems and tools to detect and prevent web application based attacks are discussed in [11, 12, 13, 14, 15].

III. LACUNA OF CURRENT SYSTEMS

Though many systems are currently present for detecting and preventing web attacks, they are often limited in scope and functionality. Many of the systems discussed above focus only on the network layer security alone. Many proposed tools can only respond to certain types of attacks. Most of the systems are also platform specific. Thus, for a developer to make a secure system, it is extremely difficult to implement the different tools across different layers and also make it platform independent. The advancements in technology such as Cloud Computing also leads to new platforms and modifying an existing security system to function on new platforms is a tedious and expensive task. Many of the existing systems provided by third party vendors are costly and also need extensive customization in order to fit the needs of the client. False alarms are also frequently generated by these systems which cause unwanted delay or resource wastage due to the responses made.

IV. PROPOSED TOOL

Our proposed system aims at creating an open source cross platform application side intrusion detection and response framework to detect and respond to web application based intrusion attacks. The system employs statistical models such as the Chi squared fitness test and Bayesian probability in order to validate the attacks and reduce the number of false alarms. Using the power of open source, the tool can be further expanded and validated with the input of the open source community. We also use only open source software and tools in the development of this framework.

Our proposed system functions on the application layer of the OSI architecture whereas most of the current systems function only on the application layer. This is represented in Figure 1.

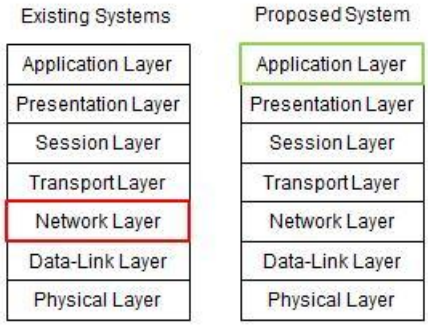

Fig.1. Comparison of existing and proposed system

Our system has a Domain Authenticator, a Detection Engine, an Analysis Engine and a Response Engine. These constituents together form our Web Application Based Intrusion Detection and Response Tool. The architecture diagram for the system is show in Figure 2.

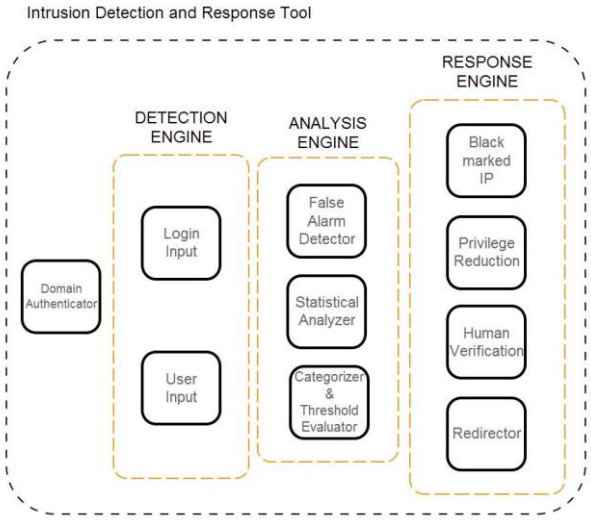

Fig.2. Architecture Diagram

The overall flow chart of the system is shown in Figure 3. The system functions by executing the login sensor module. The inputs are then parsed by the system