Project Design Phase-II
Technology Stack

Technical Architecture:

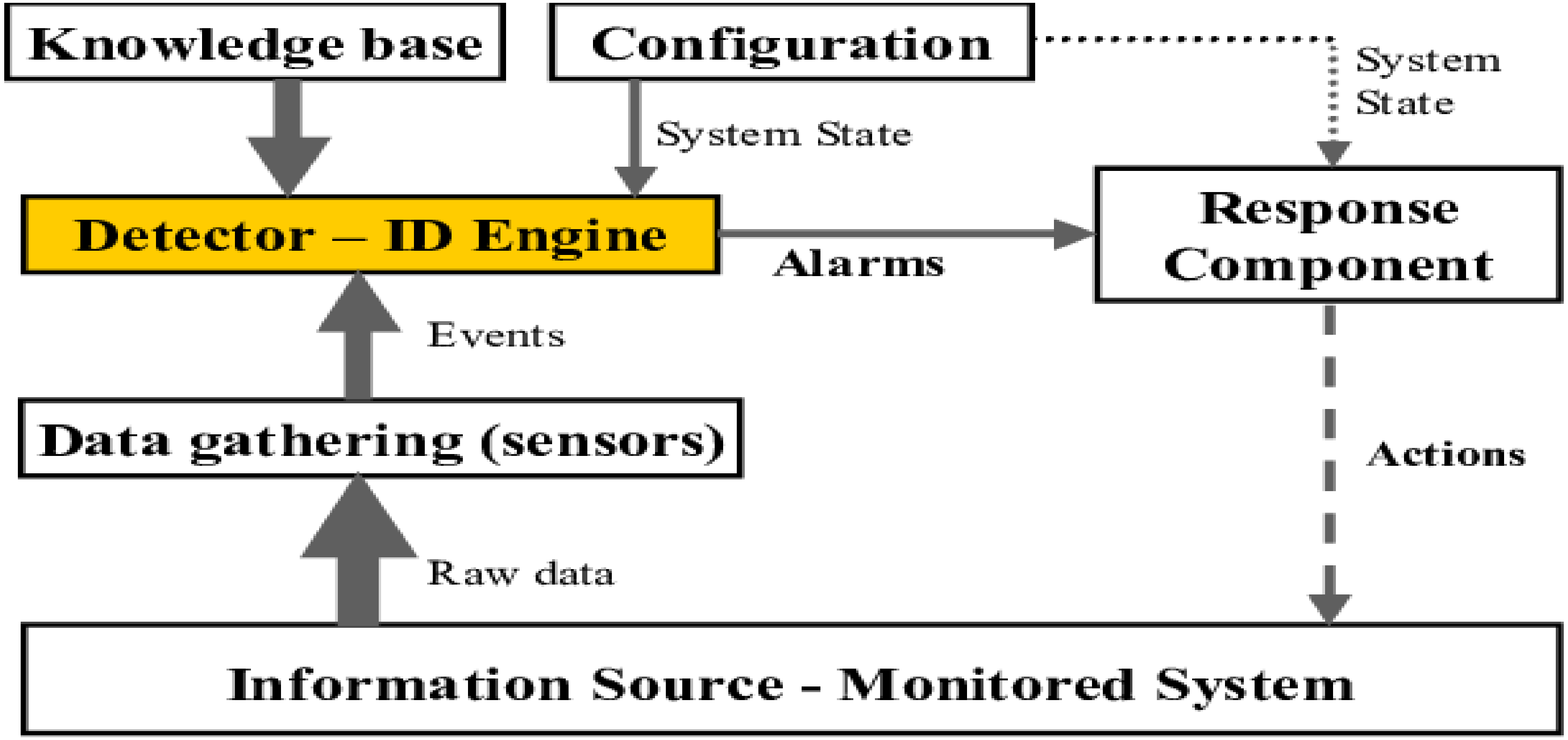

Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	How user interacts with application e.g. configure ids, view alerts, generate reports.	HTML, CSS, JavaScript, React Js etc.
2.	Response mechanism	Depending On the severity of the intrusion, application logic component can trigger various responses, such as blocking network traffic, or sending alerts to administrators.	Python, Cloud services.
3.	Alert mechanism	When a potential intrusion is detected, this component generates alerts or notifications. This alerts may vary in severity based on the perceived threat level.	Email, HTTP API service.
4.	Cloud Database	These databases provide an flexible and scalable approach to data storage and management.	IBM DB2, IBM Cloud ant etc.
5.	File Storage	It refers to storage and management of files and data, in a structure consisting of folders and files.	Python, Java, MySQL, etc.
6.	Vulnerability databases.	IDS can query databases like CVE, database to check for known vulnerabilities associated with detected assets.	Python, SQL, Restful API, etc.
7.	Firewall API's	IDS can integrate with network firewalls to automatically block or isolate malicious IP's. This might involve firewall API's like windows firewall, cloud firewall services.	SSH, Restful API, etc.
8.	Machine Learning Algorithms.	This algorithms like neural networks or decision trees help in identifying abnormal patterns that might indicate an intrusion.	Python, R, Java, etc.
9.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud Local Server Configuration: Cloud Server Configuration :	Local, Cloud Foundry, Kubernetes, Recognition etc.

Table-2: Application Characteristics:

S.No	Characteristics	Description	Technology
1.	Open-Source Frameworks	An open-source framework is a software development environment that is made available for public with its source code accessible and modifiable.	Kubernetes, Elastic stack, etc.
2.	Security Implementations	They can encompass a wide range of measures to protect systems, data, and information from unauthorized access, threats.	NIDS, HIDS, Clod-based IDS, IAM Controls, OWASP, etc.
3.	Scalable Architecture	An architecture that doesn’t require changes to upkeep effective performance when there is an increase in workload.	Elastic cloud services, machine learning, etc.
4.	Availability	It refers to readiness and reliability of the system to be consistently accessible.	Load balancers, CDN's, etc.
5.	Performance	It refers to speed of a system in executing tasks and delivering results.	CDN's, Scalability, Caching, etc