Software Architecture Assignment-2 (SEZG651/SSZG653)

SAQUIB

2021MT12266@wilp.bits-pilani.ac.in

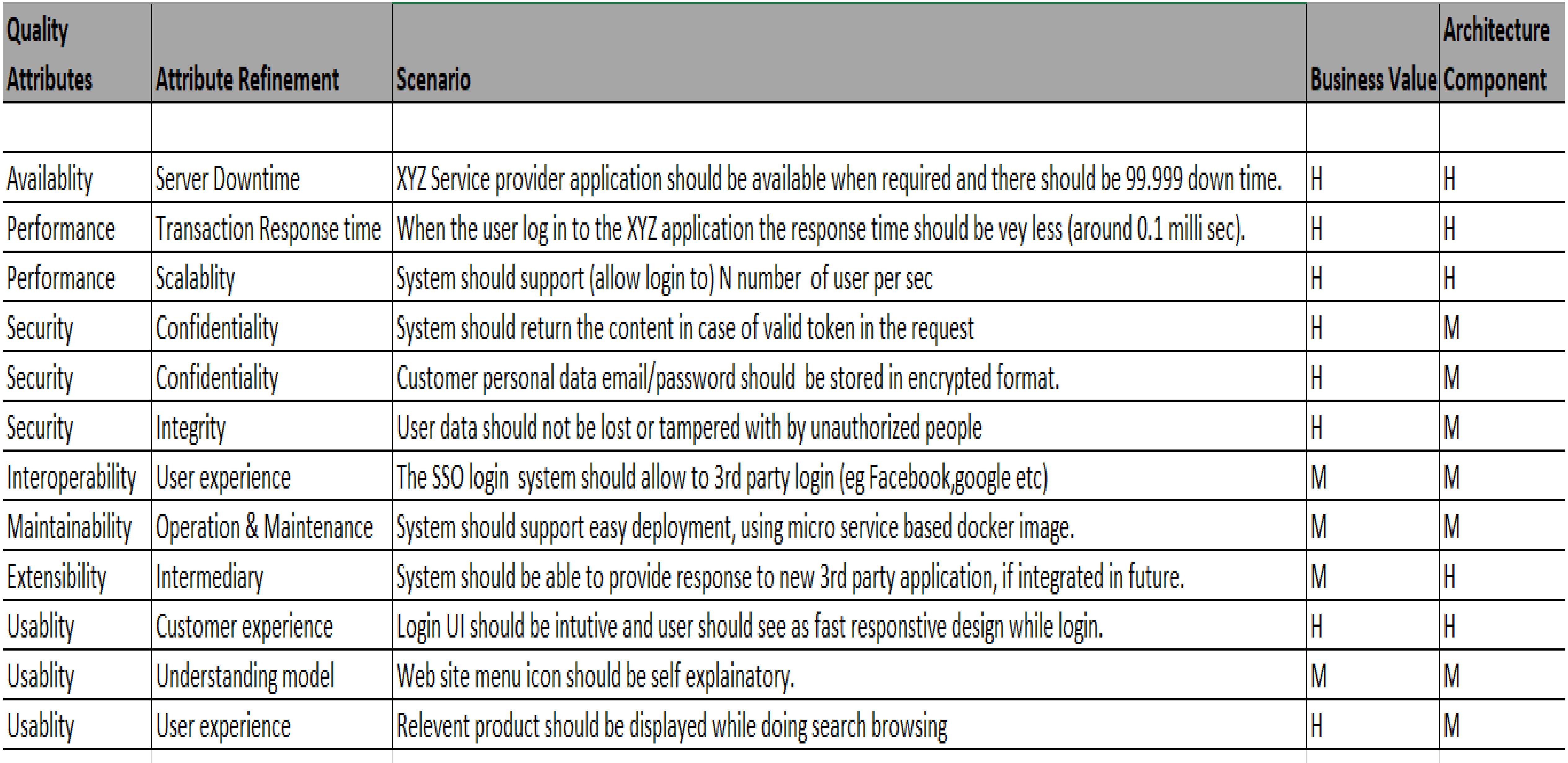
Purpose of the System

- ✓ Currently XYZ service provider having separate login for multiple XYZ service applications, XYZ partner app and XYZ web portal.
- ✓ Requirement is to implement single sign on and two factor login authentication for all the XYZ service so that user can login to all XYZ application ,XYZ partner app, XYZ web portal to the single id and password.
- ✓ Enable users for 2 factor authentication for XYZ partner app.
- ✓ Enable authentication and Single sign in to XYZ service application.
- ✓ Enable authentication and Single sign on to XYZ web portal.

Key Requirements : Functional & Non-Functional

Functional requirements	Non functional requirements
• A user data must be secure and must not be leaked to an outsider, while user entering the login information , it should not be hacked or breach in any way. • Only valid login should be allowed to enter in the system • The data entered by user should be accurate based on details end user should view the module of the application. • User need to enter login email, mobile number username and OTP password if required to login the XYZ services. • System must allow to reset the password by clicking the “Reset Password” and receiving a link to their email address. • Password should be combination of 8 character long, No space, Upper Case, Lower Case, Numeric and Special character	Performance: • System should be able to support y number of users on the big billion sales • Time taken to view the UI page after login should not be more than t seconds. • Navigation form one page to other page should not take more x seconds. Availability • The system should be completely operational at least Z% of the time. • Downtime of the system should not exceed X min Modifiability • System should be able to integrate new products without major re-work. Interoperability • ABC website portal should be viewable to chrome, ff, safari, android and IOS platform Security • Customer sensitive data stored in encrypted format Usability • Website and application navigation should be intuitive and user friendly.

Utility Tree



Quality Attributes	Attribute Refinement	Scenario	Business Value	Architecture Component
Availablity	Server Downtime	XYZ Service provider application should be available when required and there should be 99.999 down time.	H	H
Performance	Transaction Response time	When the user log in to the XYZ application the response time should be vey less (around 0.1 milli sec).	H	H
Performance	Scalablity	System should support (allow login to) N number of user per sec	H	H
Security	Confidentiality	System should return the content in case of valid token in the request	H	M
Security	Confidentiality	Customer personal data email/password should be stored in encrypted format.	H	M
Security	Integrity	User data should not be lost or tampered with by unauthorized people	H	M
Interoperability	User experience	The SSO login system should allow to 3rd party login (eg Facebook,google etc)	M	M
Maintainability	Operation & Maintenance	System should support easy deployment, using micro service based docker image.	M	M
Extensibility	Intermediary	System should be able to provide response to new 3rd party application, if integrated in future.	M	H
Usablity	Customer experience	Login UI should be intutive and user should see as fast responstive design while login.	H	H
Usablity	Understanding model	Web site menu icon should be self explainatory.	M	M
Usablity	User experience	Relevent product should be displayed while doing search browsing	H	M

Utility Tree for ASR

Quality Attributes	Attribute Refinement	ASR
Availability	**Server Downtime**	XYZ Service provider application should be available when required and there should be 99.999 down time. If server went down, it would affect the user experience which in turn effect the business.
Performance	**Transaction Response time**	When the user log in to the XYZ application the response time should be vey less (around 0.1 milli sec).For e.g. If the user searching for any consumer product on the website the search time should be minimum so that next time customer visit same website which will lead to increase in business.
Security	**Confidentiality**	When user/vendor log in to the portal using mobile , email they should see only their information and customize view. For e.g.: Add to Cart items, Recently viewed , Like products etc.
	Integrity	When user tried to login and used incorrect password thrice, alert should be prompted on mobile/email and his/her account should be locked for 15 min.

Security ASR(Quality Attribute)

- <u>Security requirements:</u>
- Security is one of the Important ASR which required irrespective to whatever domain project is being delivered.
- The main requirement for the XYZ service it provides multiple applications to the users and there should be proper Confidentiality , Integrity , Authentication and authorization implementation mechanism in place.

a) When the user login to the widget using the mobile number or email then the detail/information related to that user should only be visible.

b) If X user logged in to the Service X and have added product to cart, then only his cart information detail should be Visible.

c) If any malicious user tried to log in to your and enter the password wrong thrice then alert should be prompted to logged in email /mobile number.

Tactics to achieve ASR(Security)

Quality Attribute	Scenario (ASR)	Tactics
Security	User personal data email/password should be stored in encrypted format.	•Encrypt critical and personal data using standard protocol Like DB user Password will be encrypted using SHA256 Algorithm, sensitive data of application like password AES 128 algorithm for encryption •Access security includes identification, authentication, authorization, access control, session control etc.
	Client data should not be lost or tampered with by unauthorized people	•No direct access database by any user, all system user can access backend data through system business process with respective access rights. •Coding security includes security methods during programming of codes
	Operation & Maintenance	•Monitor all system to find exception and attacks by using Intrusion detection and prevention system. •Manage and audit system logs through a centralized log server

Performance ASR(Quality Attribute)

- Performance requirements:

- Performance is also one of the most Important ASR in e-commerce application.
- If the user has logged in to the any of the services application of XYZ the response time should be very less so that customer experience should not degrade.
- If X user has logged in to XYZ Website and start purchasing the One brand electronic product and redirect to the payment page, then the response time doing the payment should less so that the user response is positive and next time if user want to buy any product should visit same site which will lead to increase in business.
- System should perform well and response smoothly during high rush period, The system should deliver response within X second during the peak load of N tps.
- System should, able to scale in or scale out depending on the requirement

Tactics to achieve ASR(Performance)

Quality Attribute	Scenario (ASR)	Tactics
Performance	XYZ service application response within T milli seconds.	•Use Asynchronous Programming to handle the concurrent HTTP requests for maintaining session request. •Using Caching to Improve Performance •Create Proper Database Structure
	XYZ System should be able to Scale In/ Scale Out based on server load	•Fully Micro-service Based Architecture to support use AWS Elastic load balancer •Kubernetes/Container: support quickly Scale In/Out,
	System should support N number of request per second	•Use Apigee platform for developing and managing API proxies. •Use Optimize SQL query and caching techniques. •The system must be deployed on multiple web servers behind a load balancer that would round robin between each servers.

Availability ASR(Quality Attribute)

- Availability requirements:

- XYZ Service provides multiple applications and web portal , ecommerce platform, the most important characteristics is the system remain available when needed.
- The system shall be completely operational at least 90% of the time.
- Down time after a failure shall not exceed 2 hours as it is the E-commerce project so down time is proportional to the customer and if the user is not happy with the service, then it will affect business
- System should generate alert and display messages on the monitoring board as soon as service is down, so that recovery or backup mechanisms should be incorporated.

Tactics to achieve ASR(Availability)

Quality Attribute	Scenario (ASR)	Tactics
Availability	All XYZ services and application should be highly accessible if the network identity provider goes down.	•Use Active redundancy configuration wherein all the nodes (active or redundant spare) in a protection group receive and process identical inputs in parallel •Identity provider should have minimum downtime and using backup feature to always remain available.
	XYZ System should be able to detect fault, active session, certificate expiry and exception.	•Use multiple LDAP directory for certificate renewing. •Upon active session count, If one controller down authenticate with other controllers.
	Provide continuous monitoring and alerting system for any fault, downtime and exception of the XYZ services.	•Determines reachability and round-trip delay through the associated network path . •In high-availability system, monitors state of system health, SSO logs detects hung or runaway processes •Indicates to system monitor when fault is incurred in process

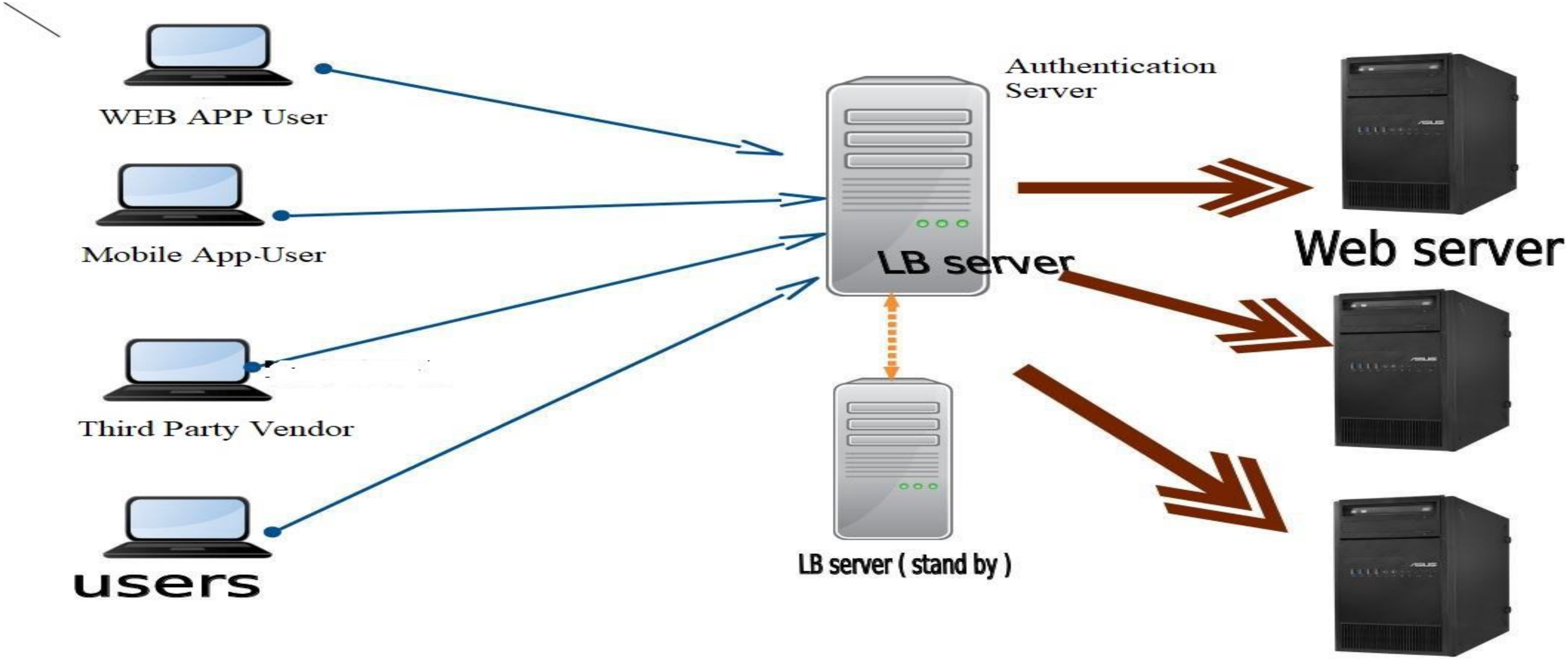
Tactics Brief Summary to achieve ASR

Goal	How Achieved	Tactics
High Performance	Load balancing, network address translation, proxy servers	Introduce concurrency; increase resources; multiple copies
High Availability	Redundant processors, networks, databases, and software; load balancing	Active redundancy; transactions; introduce concurrency
Scalability	Allow for horizontal and vertical scaling; load balancing	Abstract common services; adherence to defined protocols; introduce concurrency
Security	Firewalls; public/private key encryption across public networks	Limit access; integrity; limit exposure
Modifiability	Separation of browser functionality, database design, and business logic into distinct tiers	Abstract common services; semantic coherence; intermediary; interface stability

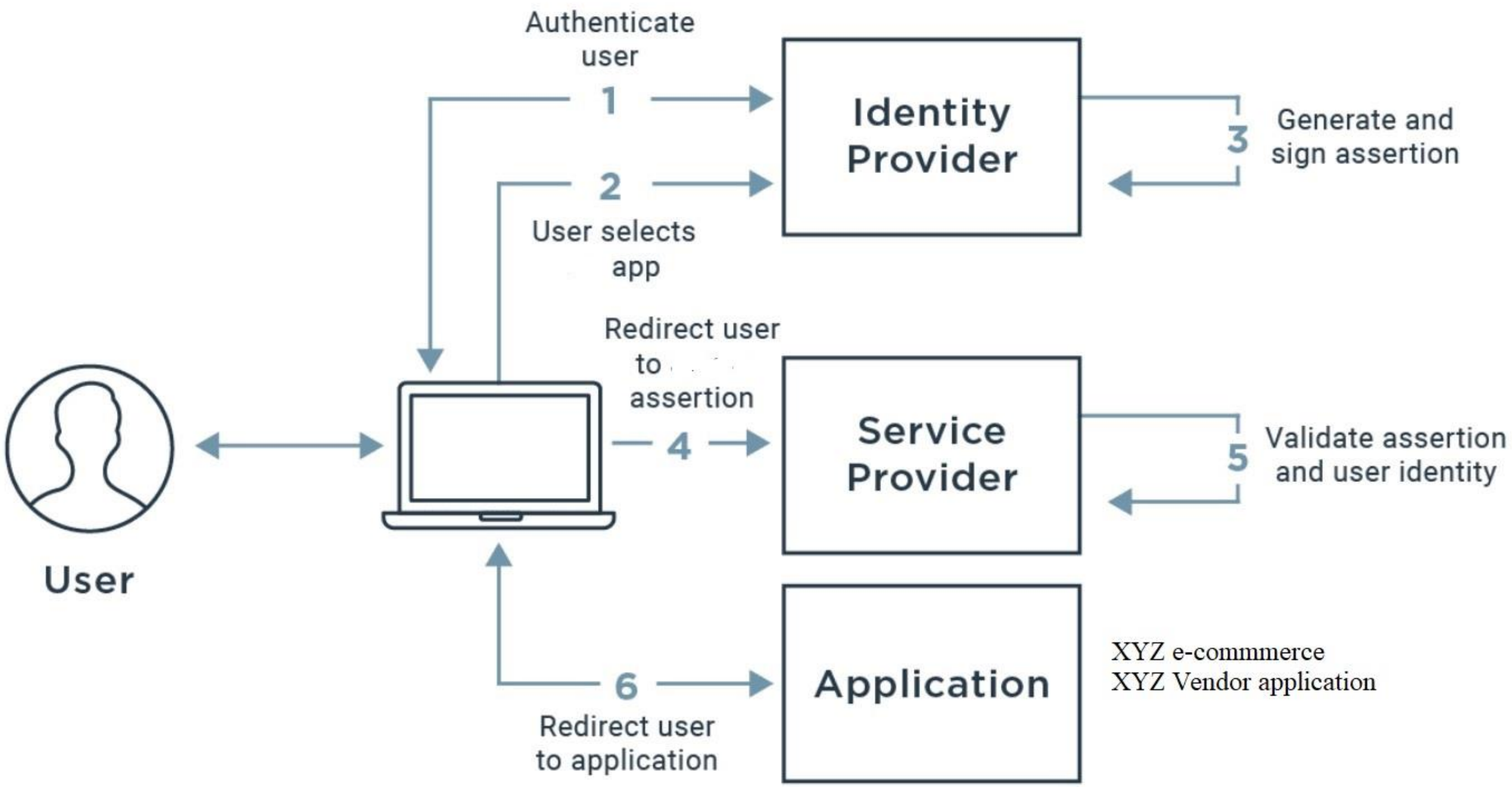
Architecture Pattern Used

- We have used client-server pattern for implementation of SSO login.
- Client server pattern is a network architecture that consist of a server and multiple clients.
- Servers are powerful and it will provide service to multiple client components
- Clients rely on servers for resources such as files, devices & processing power.
- When any user tries to login to the XYZ it request goes to ELB from there respective sso-proxies server to authentication the login validation.

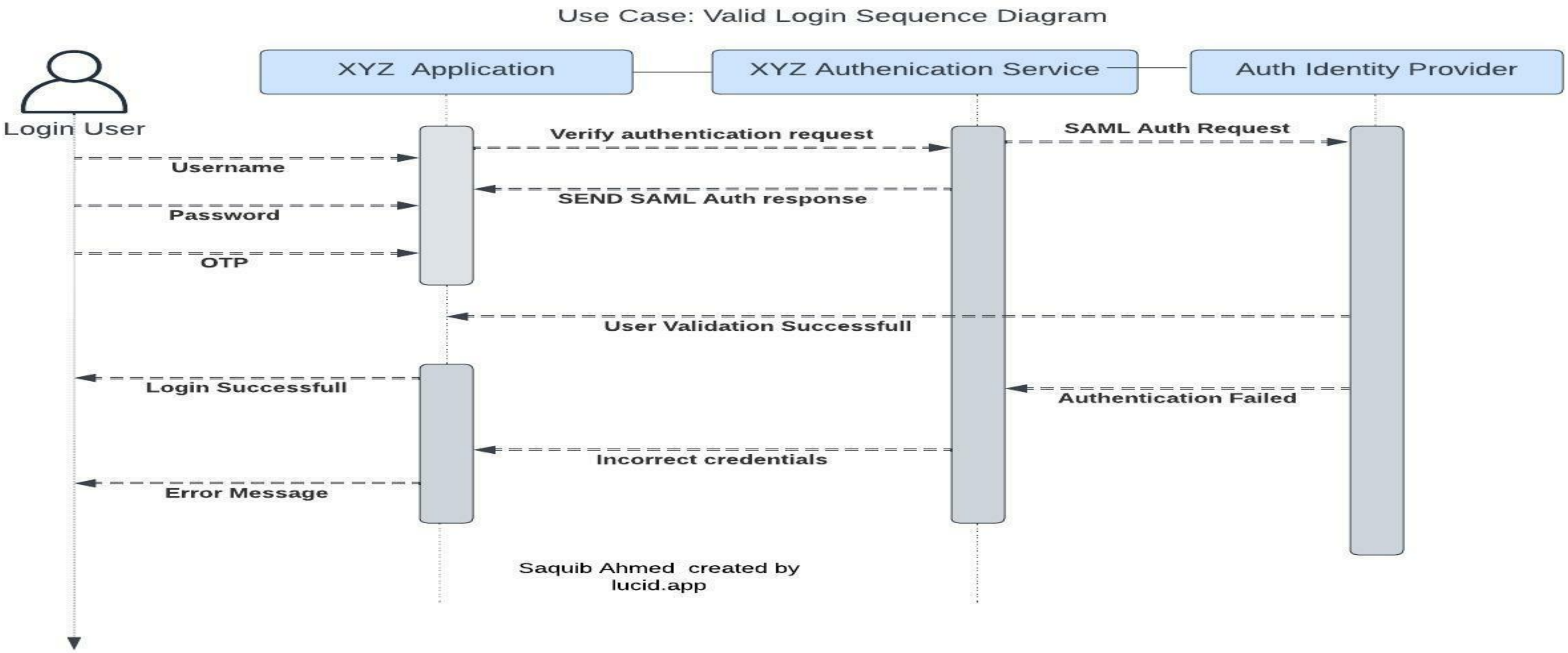
Client-Server Architecture Pattern



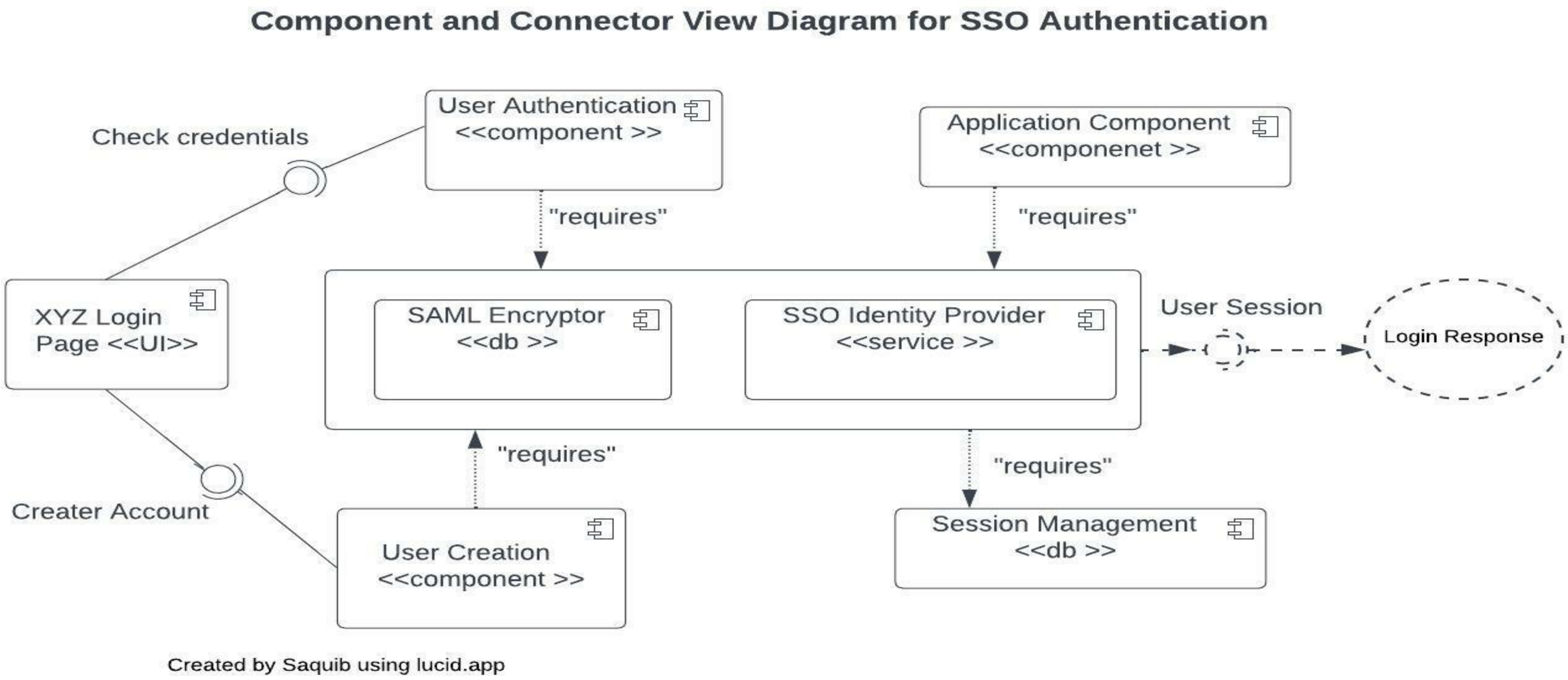
High level Architecture Flow Diagram



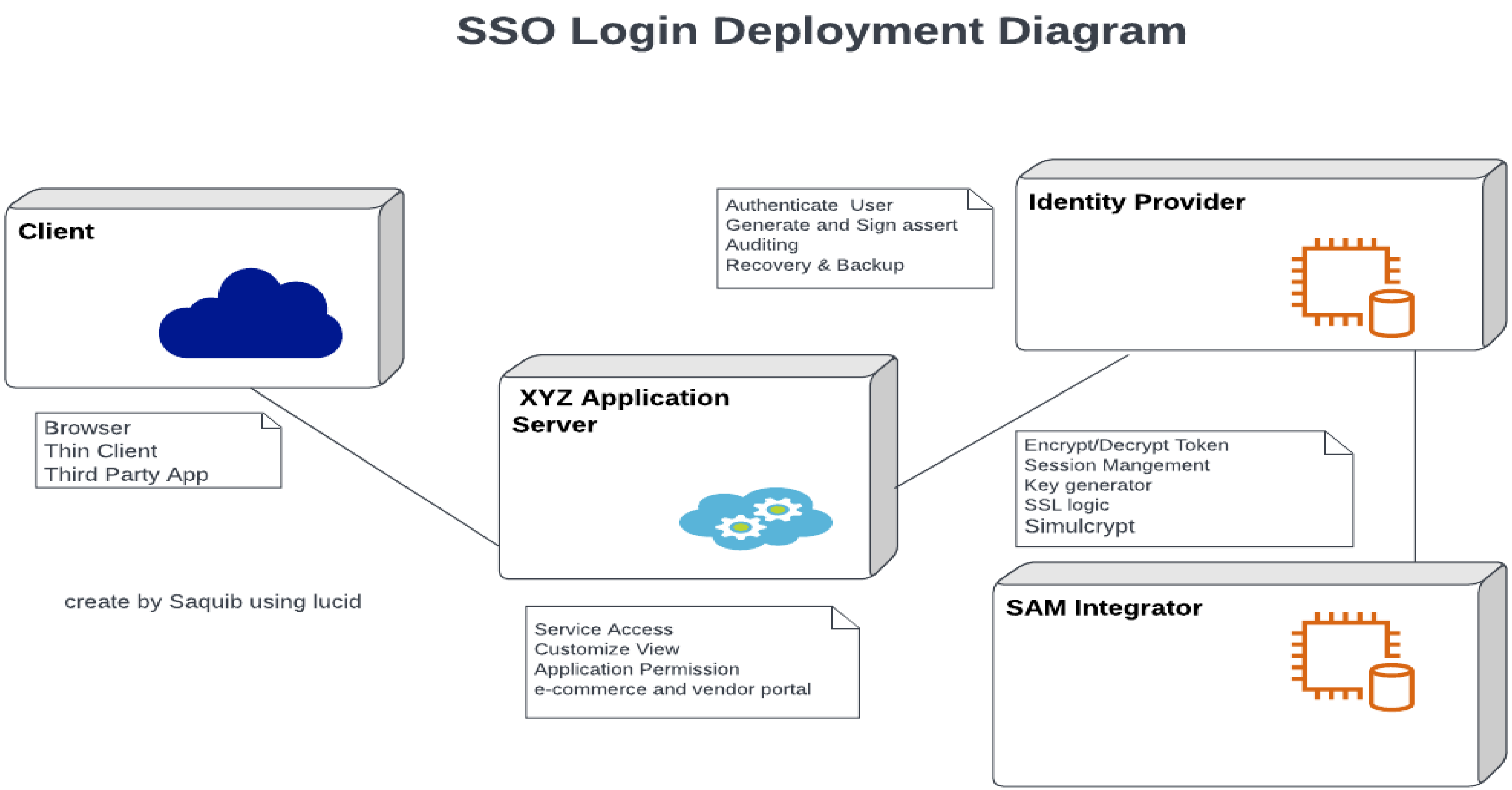
Ssequence diagram for valid login flow



Component and Connector View Diagram



Deployment Diagram



SSO Login Deployment Diagram

Client

Browser
Thin Client
Third Party App

XYZ Application Server

Service Access
Customize View
Application Permission
e-commerce and vendor portal

Authenticate User
Generate and Sign assert
Auditing
Recovery & Backup

Identity Provider

Encrypt/Decrypt Token
Session Mangement
Key generator
SSL logic
Simulcrypt

SAM Integrator

create by Saquib using lucid

System Working

1. SSO sign-up will be similar to the email sign-up flow

a) When SSO is selected but the social session is not logged in , then login prompt will be asked from which account the user want to login.

b) When SSO is selected and multiple social sessions are logged in, then would ask for which login session to use.

2 . In sign-up process starting the end user can login through the Mobile Number / Email Id . Once the user logged in the login Id the detail will be verified from the backend and once the detail are verified then the user will be logged in and redirected to the app page for which user has logged in   If the login Id and password does not match then the error message will be pooped to login with correct credentials.

3 .Forgot password – Functionally Flow (If the end user does not remember the login password)

a) User will click on Forgot Password button .

b) The button will redirect to Forgot Password page where user will enter the Mobile Number/Email Id where the otp will be send.

.

System Working

c) Once the otp is send there will timer set on the UI that user has to enter the OTP in the 30 second if user fails to do then the end user has to again click on the resend OTP button

d) Resend OTP button will again send the OTP to user via Mobile Number or Email ID

e) Once the OTP is verified the user can set the new password for login.

f) After the password is set successfully user will be automatically taken to logged in state.

4.User Logged With Unverified Email Id

a) If has logged in with an mobile number & provided Email ID which user forgot to verify within 3 days of duration.

b) On entering the email id otp will be send to the end user email id . Email ID will be verified, and user will be logged in.

Key Learnings

- Know how to define system requirement and identify ASR.
- Got the idea of how Availability, modifiability, Performance, Security scenario tactics used practically.
- On personal experience, If the architecture is properly design , it help us to understand the project easily and enable to speed up the development activities.
- It help us to see the reduce the risk factors, analyze the cost of the project ,and identify other critical requirement which might be overlooked if the architecture not design properly.
- By designing proper architecture, all quality attributes can be taken care which led us to deliver customer centric, aligned with business requirement project.

THANK YOU