modellazione non sempre si è a conoscenza di tutti i dettagli per cui deve essere sempre possibile ritornare sull'aspetto sotto analisi in un secondo momento per poterlo approfondire ulteriormente. La figura che segue riporta l'esempio di un diagramma iniziale che mostra l'architettura di una applicazione con alcuni dettagli.

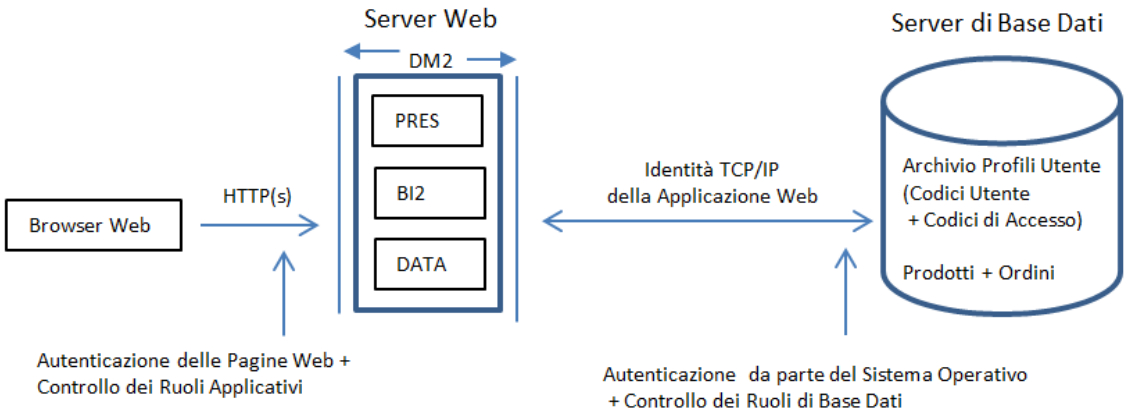

Figura 8 - Esempio di disegno architetturale di una applicazione

In generale il disegno architetturale deve evidenziare i seguenti elementi:

- Topologia fisica e logica dei componenti: il collocamento dei server in rete (Intranet, Extranet e accesso a Internet). Iniziare con le topologie di rete logiche, per poi visualizzare le relative topologie fisiche quando si dispone di tali dettagli. È possibile aggiungere o rimuovere le minacce a seconda della scelta di topologie fisiche.
- Livelli logici: il livello di presentazione (front-end), il livello di business (back-end) e i livelli di accesso ai dati. Successivamente occorre rifinire per includere, una volta noti, i limiti fisici del server;
- Componenti chiave: i componenti importanti all'interno di ogni livello logico. In questa fase è possibile includere i limiti reali del componente e di processo una volta conosciuti;
- Servizi chiave: i servizi importanti. Una volta noti, da mostrare come processi;
- Porte e protocolli di comunicazione: i server, i componenti e i servizi che comunicano tra di loro e come lo fanno. Da mostrare le specifiche dei pacchetti dati in entrata e in uscita, una volta individuati;
- Identità: le identità utente principali usate all'interno dell'applicazione e gli eventuali profili di servizio rilevanti;
- Dipendenze esterne: le dipendenze dell'applicazione da eventuali sistemi esterni. Elencare queste dipendenze è utile per individuare possibili vulnerabilità che potrebbero insorgere in un secondo momento se alcune assunzioni fatte inizialmente sul generico sistema esterno dovessero risultare non più vere o in qualche modo cambiate.

È importante revisionare il disegno del sistema nel corso del tempo per verificare se tutti gli elementi individuati siano ancora come descritti, se devono essere cambiati o se hanno bisogno di un ulteriore livello di dettaglio.

6.1.2.1 Identificazione dei Ruoli

È importante identificare i ruoli all'interno dell'applicazione, ovvero, chi può fare cosa.
La fase di identificazione dei ruoli è utilizzata sia per determinare ciò che dovrebbe accadere (accesso alle risorse autorizzate come stabilito per lo specifico ruolo) che per determinare ciò che non dovrebbe accadere (accesso a risorse per le quali non si ha l'autorizzazione).
L'assegnazione dei ruoli deve essere centralizzata e a ciascun ruolo deve essere associato un profilo 'autorizzativo' che regolamenta i comandi, le transazioni e gli accessi ai dati.