Dalton Murray, Norhan John

Systems Analysis and Design

INT 6123 – Systems Analysis and Design

Dr. Andrew Makar

November 5, 2023

**Case Study 2**

**Develop the domain class diagram (50 points)**

The case study has identified several entities including the contractor, the project, project activities and the actual time card.

For each of these entities, define the data structure and the field types.

* Contractor
* Project
* Activities
* Time Card

A contractor is an employee of TekSystems who does work at Makar Motors.

A contractor has at a minimum a first name, last name, email address, phone number and hourly billing rate.

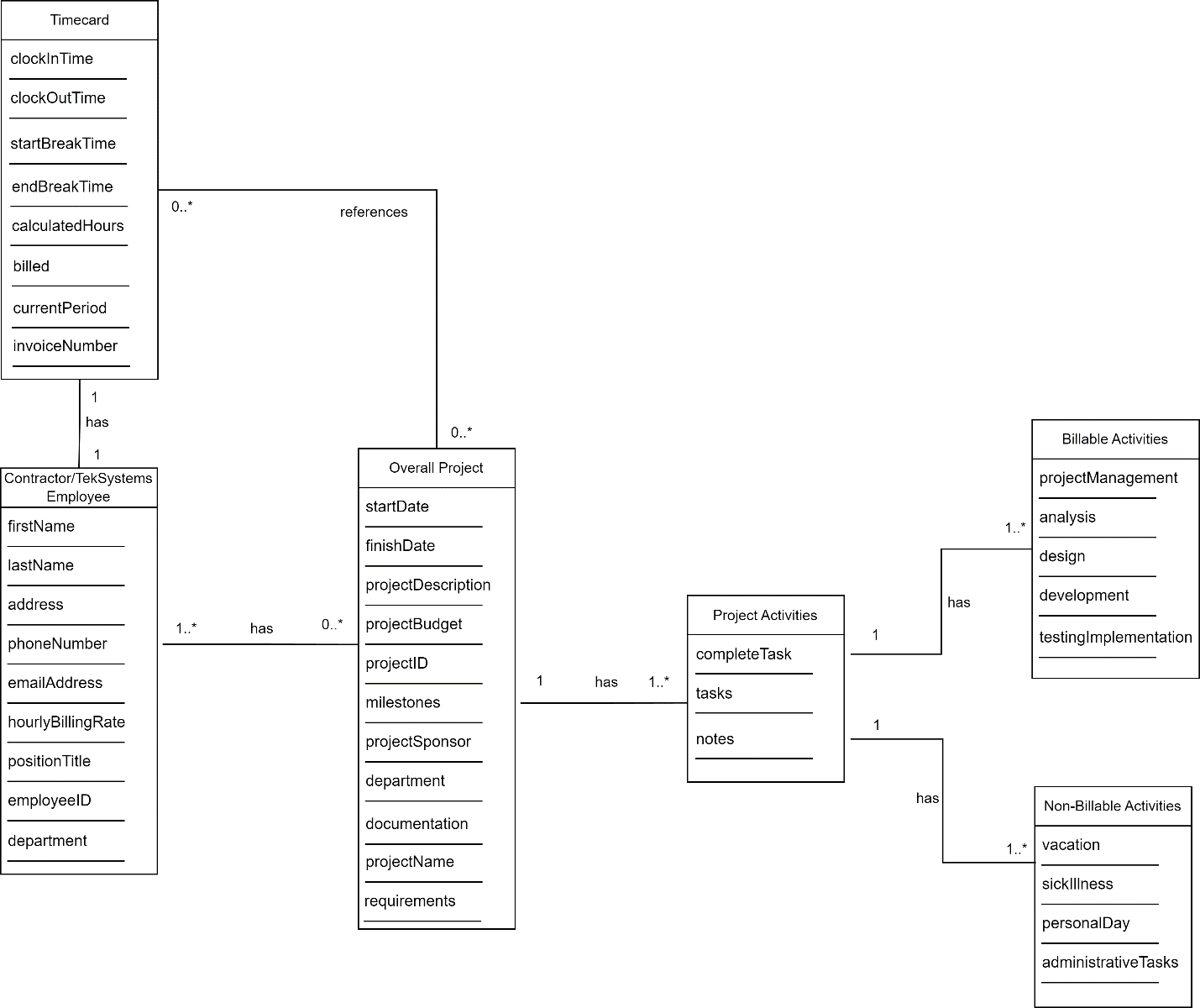
A project has a start date, finish date, project description, project budget and a project id.

Project activities incude billable and non-billable activities. Billable activities include Project management, analysis, design, development, testing and implementation. Non-Billable activities included vacation, sick/illness, personal day, or administrative tasks.

Refer to the time card example for field definitions.

Please add any additional fields based on your understanding of the system context.

PNG:

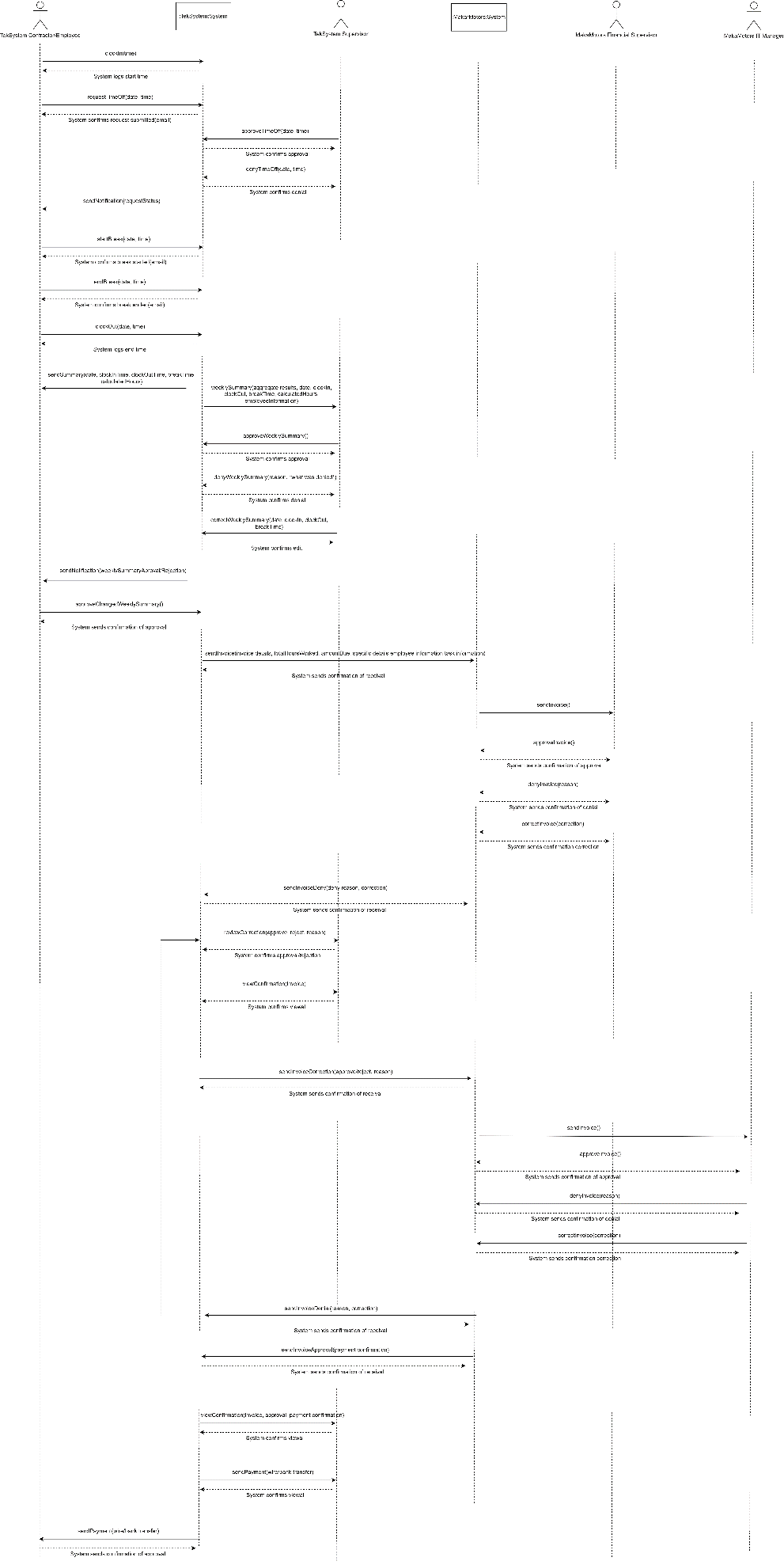


PDF: Attached separately.

**Develop a SSD for Mass Time Approval (20 points)**

* Develop a SSD diagram and include the notation for Mass Time Approval and Mass Time Approval rejection.
* Identify any methods or functions that would be used for future development

PNG:



PDF: Attached separately.

**Design Access Controls for the application (30 points)**

**Describe the authentication process to log into the system.**

When you first go to the website you will click login. Each page will have an SSL/TLS certificate. You will enter your username and password. The username is automatically generated by the person’s name (Dalton Murray -> dmurray), if there’s multiple people a number is added onto the end. A default password is made for initial account creation, and then the person resets it to their own password. The password must be at minimum 12 characters including capital letters, numbers, and special characters. The password will be hashed locally and sent to use to compare to our hash in our database in an end-to-end encrypted manner to ensure higher security. After logging in, it will then send a code to their authenticator or text them a number or email them a verification code. Once they login they can then access their usual systems. For people who are higher up (C-Suite and directors, etc.) in the company, we will also have strict authentication requirements, it will require their username, password, phone code, and hardware authenticator (security key). On top of all of this, we give each employee the ability to add and change their security requirements, for example if they also want to use a hardware authenticator/security key, or have specific location locks put in on their account. Upon a failure the system will log the IP of the person attempting to login and calculate an approximate location then email and text this failure to authenticate to the stored email address and phone number. Upon 3 attempted failures the system will suspend/lock their account and send an email and text upon this, this will also get sent to our IT Security/Cybersecurity team. Upon system failure, a backup system will take in place for authentication purposes, upon the backup failure the employee will not be able to access the login page and will get automatically redirected to a status page with the current status (maintenance, system outage, announcements such as working on, known error, etc.).

**Develop a use case for multi factor authentication using the use case template from previous modules**

|  |  |  |
| --- | --- | --- |
| **Use Case Name** | Multi-Factor Authentication | |
| **Scenario** | The company wants to ensure that all employees have secure accounts and have the ability to use multi-factor authentication and have the ability to customize their security options to ensure a secure yet quick authentication process | |
| **Triggering Event** | The employees want to access a system that requires multi-factor authentication | |
| **Brief Description** | This use case shows how a user can log into the company systems using multi-factor authentication, which requires the user to identify themselves in 2 or more ways via email, text, authenticator app, hardware key, and other offered options in the future | |
| **Actors** | Makar Motors, Employees, Financial Coordinator/Department/Acting coordinator, IT Manager, TekSystems supervisors | |
| **Stakeholders** | Makar Motors, Employees, Clients | |
| **Preconditions** | The person must work for Makar Motors or TekSystems, they must have at minimum two-factor authentication added to their account | |
| **Postconditions** | The person is securely logged into the system | |
| **Flow of Activities** | **Actor** | **System** |
| 1. Goes to the login page  2. The person enters their username and password  3. Selects next option of authentication (email, text, authenticator app)  4. Receives the email, text, or checks authenticator code  5. Inputs email, text, or authenticator code into login  (Optional) 6. Third/4th, 5th, nth level of authentication  7. Safely accesses the system | 1.1 Displays the login page to the person  2.1 (Internal person computer) Hashes the password  2.2 Sends the hashed password to the system  2.3 Compares the hashed password to the existing hashed password in the database  2.4 Display prompt for next level of authentication (email, text, authenticator app)  3.1 Performs action  - Send email  - OR Send text  - OR Await entry for authenticator code  5.1 Verifies second method of authentication  5.2 Displays failure/success  (->) 5.3 Upon failure will log IP, approximate location and email and text verified/stored email and phone number  (->) 5.4 On the third failure will suspend/lock account, send email and text to employee and IT Security/Cybersecurity team  6.1 Verify next level of authentication (hardware/security key, etc.). |
| **Exception Conditions** | 2.3 The hashed password can fail to compare to the existing stored hashed password  5.1 The second method of authentication can fail to verify  6.1 Failure for third, fourth, fifth, nth level of authentication | |

**Identify time keeping system users in the case and categorize the users according to Unauthorized, Registered and Privileged users. Add any roles or actors not previously identified in the case.**

The additional time keeping system users are: Financial Coordinator/Department/Acting coordinator, IT Manager, TekSystems supervisors, TekSystems employees.

Unauthorized users: Anyone who does not work for TekSystems, or Makar Motors

Registered users: Employees of TekSystems and Makar Motors

Privileged Users: Financial Coordinator/Department/Acting coordinator, IT Manager, TekSystems supervisors

**From your reading, you know you will need an HTTPS certificate. Research the SSL certificate costs and identify 2 options for installing SSL into the solution.**

Today, there is no reasoning to pay for an SSL/TLS certificate, however, there used to be a few years ago. The first option for installing an SSL/TLS certificate is using Cloudflare (<https://www.cloudflare.com/>). Cloudflare can be completely free, or paid for, however, their SSL/TLS certificate is free. They are able to easily install it for you as long as you point your name servers to them. The second option we have researched is Let’s Encrypt, they also offer completely free SSL/TLS certificates, although, require a little additional setup compared to Cloudflare (<https://letsencrypt.org/>). Both Cloudflare and Let’s Encrypt make up a majority of SSL/TLS certificates today, with AWS providing an additional large percentage.

**Describe the backup and recovery plan for the system**

For backup, we will implement a multi-layer system to try to ensure that the system never goes offline. We will have standby servers in place that are ready to get traffic diverted to it so they employees can always log into and access the systems. In more technical details, we will have a RAID array for storage/data, however, a RAID array is no longer considered a true backup plan today it is only considered an availability backup meaning that if a drive fails the systems are still accessible and not that for true backup purposes, although many people still consider it to be for that use and it technically has some truth to it. We will ensure that we have full offline backups available of all systems (taking a copy of it and then storing the harddrive/SSD in a secure location). We also will have secured cloud versions of the backups to ensure that we are practically guaranteed a full backup of our systems. The cloud backups will be completely automated. For our recovery plan specifically, we will ensure that our backups are usable and working, we will do manual checks of them frequently to ensure the integrity of the backups, as we are aware they many companies believe they are performing backups just for something to go wrong and then when they need their backup, they are unable to actually recover their systems by using the backup.

In addition to our standard backup and recovery plan we will revisit it quarterly to ensure that it is up-to-date with industry standards and practices. By doing this, we are making sure that what we are doing is the best way of handling backups and recovery.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

*Dalton Murray, Norhan John*