Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security
Assignment 3
Software design document

Group Members: <Fabian Dacic>, <Yuyao Duan>, <Fredric Eriksson>, <Fang Fang>

Table of Contents

1. Introduction

The IT system plays an important role for modern business organizations. To reach the management goals, companies need to adapt the state-of-the-art information and communication demands and build up an efficient and secure software system. Based on this understanding, this report aims to provide a package solution to the focal company – Loco News to improve the overall security and efficiency of the software systems.

First of all, this report will give an overview of the current IT systems of the company. A background analysis based on applying existing theoretical frameworks will be given in order to clearly present Loco News' system flaws and management issues, which the categorized problems will help to design the new software architecture. Furthermore, a systematic analysis for the planned new system will be given in order to establish a reliable guideline for the implementation of the new software architecture. A general overview of the system design including constraints and risks will be presented to achieve a secure, reliable, and efficient project of information management. Based on the above investigation, a practical IT solution will be given to Loco News in order to adapt its expanded business and the management requirements. The new software system will target appropriate hardware, software, and network architecture, which the new implemented architecture will focus on improving the performance of security and privacy. In the end, a simulation demonstration of the proposed application will be provided to verify the actual effectiveness and efficiency of the new design.

1.1 Purpose

This report aims to provide a practical and effective package solution to the software system of Loco News. Due to lack of professional knowledge, the company's current IT system cannot sufficiently fulfill the needs of business expansion and information security. Based on this understanding, a comprehensive analysis of the problems and risks of the current software system will be given to the customer to understand the urgency of implementing the new system. Based on the recognition, this report will suggest a new plan to Loco News' IT architecture and convince the customer through demonstrating the simulation of the system operation to prove its feasibility and effectiveness.

1.2 Scope

This document will present a practical software architecture and design for Loco News in order to realize a secure and reliable IT management system to adapt the expanding business requirements. The planned system will take the place of the existing one with better organizational structure and

safety performance. The new IT architecture design includes upgrading hardware and software, reorganizing the network and databases, and applying effective management procedures. Based on understanding the security flaws of current software systems, the proposed outline will achieve a more integrated and structured software architecture with high secure performance. Through applying new software, hardware, network as well as data management architecture will help Loco News to protect data and communication security. By implementing the new management approaches, Loco News could handle the growing needs of new business models. The objectives of this implementation involve safe and efficient network (wired and wireless), integrated digital office (operating system, encrypted cloud services, user access management, system and application access control, security policies), physical environmental security (servers' placement, mobile devices control, office equipment access control), effective data management (confidential storage of information, database access control, data tracking).

2. Situation analysis

Software architecture plays an important role in modern enterprises. To establish an effective system, there are a series of components, relationships, and how the components interacting with each other should be considered in advance [1]. According to "Software Architecture 5-Dimension Model", software architecture should include business strategy, design, quality attributes, IT environment, and human dynamics [1].

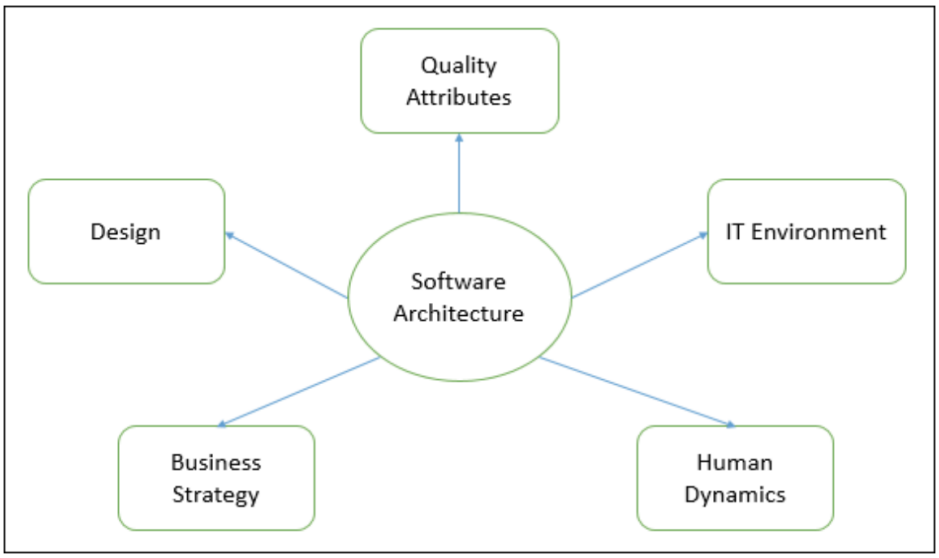

Figure 1. Software Architecture 5-Dimension Model [1]

Based on this understanding, the deficiencies of Loco News' current IT system can be assessed by this framework. In order to fulfill the need for business expansion, Loco News should attach importance and implement new management strategies to human resources (related to human dynamics), quality attribution, and IT environment.

2.1 Human resource management

In terms of human resource management, Loco News currently have the following issues needing to be improved: first of all, the background information shows that the company only has one person (the CTO) who is responsible for handling all IT technique issues (including both hardware and software) without extra staff support which can be a potential issue for Loco News to adapt the management demands of expanding business and the new software system planned to be applied. Furthermore, Loco News should review its current policies regarding confidentiality agreements. From the interviews with Loco News, we consider that more specific confidentiality agreements should be prepared to meet the security demands of the new software architecture.

2.2 Quality attribution

With respect to the dimension of quality attribution, the current IT system of Loco News has not been properly applied with ISO 27000 which is a security flaw for its software system. Since the news industry could involve a huge amount of information which should be properly handled, the lack of ISO 27000 family will weaken the organization's capability to manage sensitive information [2].

2.3 IT environment

Regarding the IT environment, Loco News by now has potential issues in terms of the following three perspectives including hardware, software, and network. Insufficient hardware management is mainly related to the server. The information shows that the basement for server placement sharing with another company could lead to potential security risks if no additional security measures are taken. Moreover, the server room lacks a proper uninterruptible power supply (UPS) system to handle unexpected power failure, since data loss caused by power outage will bring huge losses for the company. In addition, the current management strategy of using printers should be altered to improve both efficiency and safety. Printing with USBs will bring safety omissions such as spreading virus and malware among the IT system which also cannot fulfill the managerial requirements such as data tracking (what has been printed), authority management (does the user have authority to use certain printers) etc.

The current software system of Loco News has security problems as follows. First of all, the background information shows that all employees have full administrative privileges to their PCs which can be considered as a potential risk factor for organizational security. Giving users full admin privileges will put Loco News' network environment at risk [3]. This is due to the fact that with admin rights users will have full ability to download, install and execute unapproved software without supervision; configure system settings which may lead to rolling back to security changes and editing the registry – an unstable OS; and view and edit any file on the computer including the files belonging to other users which will lead to internal security risk [3]. Beyond this, the software flaws such as inconsistent and outdated software (Maverick and Windows 8), unspecified versions of the operating systems – UNIX (need to upgrade for security), and the outdated software/OS for servers (e.g. VMWare with SBS 2003 & Windows Server 2012, need to upgrade to improve security and functionality).

The network of Loco News currently remains management omissions consisting of server management and network security. First of all, the company is absent from general server management including physical protections (access protection to the server room, video surveillance, lasers, bio-metrics etc.) and environmental protections (fire extinguishers, fire alarms, and air conditioning

system for both humidity and temperature). Moreover, the servers include several different repositories for different information which should be integrated in order to achieve better security performance. The information should be classified based on different sensitivity and access permissions, and users should be authenticated to access the data. In terms of the network security, Loco News lacks proper management for employees using personal devices in the company which could lead to hardware failures, viruses, and malware attacks. To achieve the latest security performance of wireless networks, upgrading of the existing router and Wi-Fi repeaters to adapt WPA3 (2018) standard as well as integrating multi-factor authentication should be taken into consideration which can effectively prevent brute-force attack [4]. Besides, all information and data within the organization should be handled with encrypted methods no matter the size of the data. The non-encrypted free cloud service should be abandoned in order to fulfill the safety requirements for the expanded business.

3. System overview

In this section, the system's overview will include principles and strategies that will serve as guidelines and aid throughout the project. There will be information that will be beneficial during the implementation of the structure of the system, its life cycle, maintenance, execution and completion of the project.

In reference to the previous section, there are areas such as the IT environment and the quality attribution which definitely need improved alternative guidelines and principles that will need to be implemented throughout this project. For example, every member of the organization having full admin privileges on the devices and network of the organization poses a great physical and virtual hazard therefore changes in the guidelines and principles are necessary. The main principles and strategies that are going to be used will be based on the **ISO 27000** family of certifications which provide the best recommendations on information security management and management of information in the context of a system. In addition to the certifications, **frameworks** examples include those related to the software development tools from Microsoft such as Visual Studio 2019 with ASP.net with the database being based upon Microsoft SQL Server Express 2019 with operating systems for Windows Servers version 20H2. Said frameworks will be helpful due to the fact that they support organizing, securing and monitoring data including assorted information of the organization could potentially aid the project. The recommended programming language for the establishment of the system and project in general is C#. The reason why C# is being recommended is that it is relatively easy to deploy, and it is a language that has a similar syntax to Java which is quite beneficial development wise [5]. It is worth labeling a disclaimer that the aforementioned elements are not solutions however rather considered as inspiration and support for the project and that in the next section, there will be specifications and recommendations regarding such details. Certain security control clauses include however are not limited to: information security policies, organization of information security, human security resources, asset management, and so forth [6].

Aforementioned aspects of security clauses will provide guidelines that will provide protection in both physical and virtual elements of the system. Sole and full dependency on the ISO 27000 family of certifications is not advised due to the fact that there may be aspects such as policies and agreements that acquire to be flexible for various geolocations due to governments and juridical reasons which in said case a more viable approach would be for the organization to develop a certain number of its own guidelines. Advertisements to security control clauses, the main security categories and controls in the certifications mentioned in certifications are suitable means of beginning the process and implementing them in the system.

The requirements of this system are best represented by the following diagram:

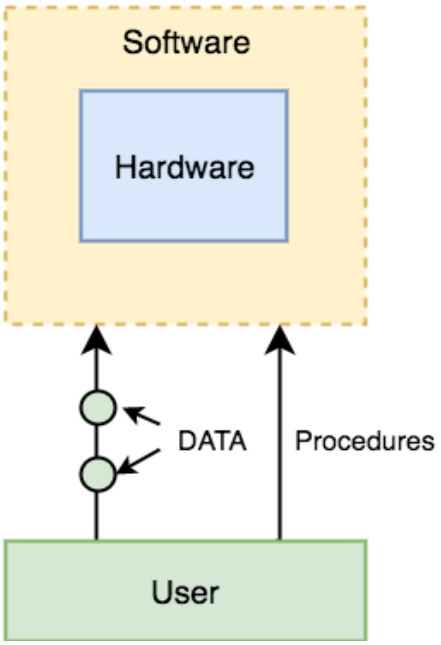

Figure 2. System diagram [7]

According to the diagram, the system requires user driven features that enable secure and efficient management, visibility, and editing of the data and assorted information through authentication and authorization. The system also requires properties such as compatible and secured hardware, and various login forms for example user credentials (i.e. username-password) to be used for insensitive access to the data and assorted information of the organization whereas user credentials (i.e. fingerprint reader) and biometric security measures intertwined are to be used when accessing sensitive information or aspects of the system, a suggestion that is to be considered. It is of most importance that throughout the development of the system and this project as a whole that error trapping or exception handling is conducted such that errors are propagated to a manageable and low risk-assessed level in which they can be handled by the development team of the organization.

3.1 General overview

The system context, design and architecture of this project consists of a hybrid between what is known as data management (DM) and content management system (CMS). The primary use of these systems is readability, managing the creation and modification of content which in this case is going to be both physical and digital of the organization. This is best explained by the following diagram:

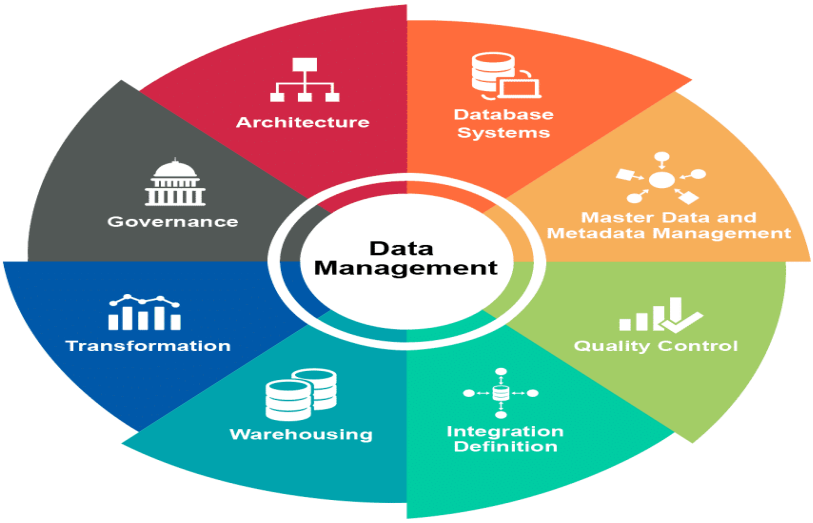

Figure 3. Diagram of a system context of a DM/CMS [8]

That mentioned, the main design approach and goal of the system that will be developed during the project is to provide a product that is secure, extensible, reliable, efficient and dynamic in the aspects of protecting data both physically and virtually in addition to handling and browse the content which is the data and assorted information of the organization. The product's main audience are the organization's members (employers and employees) and will be appropriate for private users. The system which will be indirectly or directly available considering the authorization and authentication with an approach such as an executable application or web application that serve as a gateway to the data and assorted information, the users should be able to perform various functions based on the privileges set by executives, security consultants and partners of the organization depending on the circumstances and guidelines that will be implemented as progression is made.

3.2 Assumptions

Considering the issues that are previously mentioned in the situation analysis section regarding the IT environment, quality attribution and human resource management, assumptions being made at early stages of the project are quite problematic due to the fact that the requirements and demands might be modified throughout the progression of the system and this could result in being time-consuming and costly. The three design principles that can be followed are DRY (don't repeat yourself), YAGNI (you ain't gonna need it) and KISS (keep it stupid simple) [9]. Functionalities should not be added unless deemed as necessary and they should not be complex when they can be simple for both the users and developers. The basic assumptions that can be noted are that the organization possesses the necessary resources (crew, material and facilities), economical resources (budget and financing), consistent schedule, a flexible and agile software development environment, minimal collision between different platforms and infrastructures. An example architecture that can be followed or function as an inspiration for the system is the .NET framework developed by Microsoft or other frameworks such as the SQL Server one.

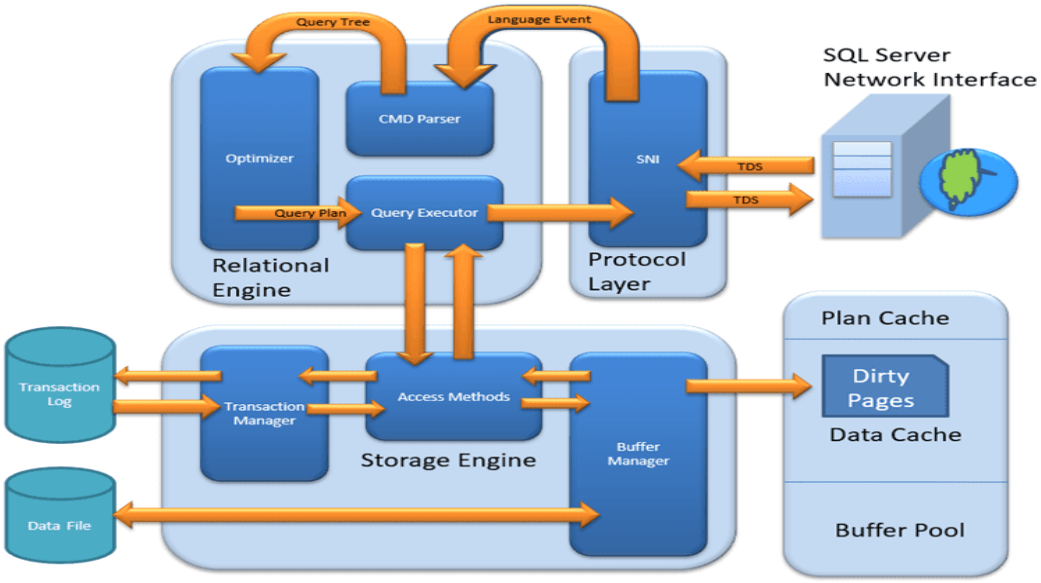

Figure 4. SQL server example architecture [10]

Assumptions about the software and its use will be that the product is expected to function on a daily basis, have security based on risk-assessing the most probable threats while having a contingency plan in case of a breach. Maintenance and upgrades must be a consideration.

3.3 Constraints

The majority of the constraints of the system's design relate to as more functionalities are added to the system, the result will be that speed and performance of the final product will most likely be affected. Refer to aforementioned design approaches such as YAGNI in which states that functions should not be added unless deemed as necessary. Programming language constraints regarding C# include code compiling due to the fact that it is based on the .NET framework hence it will not be a flexible language if there are any changes to the system as a whole, code-compiling is a double-edged sword because the code is compiled even if there are minor changes, and speed is impacted significantly hence why C# is not particularly fast [5]. These are various constraints regarding C# and should be kept in consideration throughout the project. Hardware constraints may include storage (there is an unspecified amount of the data and assorted information that the organization possesses therefore must be taken into account before the actual implementation of the system), and the layout of the devices in reference to the situation analysis regarding IT environment which will need to be reviewed as in the early stages of the project. A global limitation that has plagued the world as of currently is the pandemic in which due to safety regulations, communication will be mostly affected if done remotely and therefore time-wise, the design phase of the project could potentially take longer than expected.

3.4 Risks

There are various risks to be considered during the progress of the project. Risks such as inevitable changes in customer product strategy priority and implementation, endless changes of the requirements, physical and virtual, for the system, and operational risks. Mitigation strategies include a proper analysis of the situation as a whole and different component of the avoidance of risks by modifying the parameters of the system, continuous monitoring of both the team and potential risks that might arise during development and testing, last but not least, formulating plans in removing certain risks. In addition to analyzing the components of the project, it is advised that a risk-assessment for various hazards be conducted so that defenses can be established around the perimeter of the project as a whole. Those are the most common mitigation strategies when operating a project of this size.

4. System design

The new application to support the business processes (called TINFO in this report, abbreviation for "CEO: we need to keep better track where the information to write our articles comes from") that is under development should be based on a modern and secure platform to meet present and future requirements.

Information about TINFO according to Loco News Program Security Practical work #3, 1DV700, HT20:

- Where the information comes from
- Quality of different sources
- Volume
- Type of information
- Cost associated with getting the information
- TINFO can be hosted at own servers or in the cloud

General assumptions of design requirements for TINFO:

- Simple data model (database) based on the above information:
  - Table 1: Sources (very sensitive information)
  - Table 2: Cost
  - Table 3: Types of information
  - Table 4: Classification of information
  - Table 5: Sensitive information
  - Table 6: Roles
- Security is the top priority and the special interest:
  - All network communications should be encrypted, even for those accessing directly via LAN, no plaintext should be transmitted for communications
  - Authorization and authentication should be applied
  - Validation and input control of data
  - Auditing and logging
  - Production environment separated from development environment
  - Application, database, encryption keys and LDAP (or AD) should be separated from each other
  - Deployment of modifications to TINFO should be done in a structured and controlled way
- Users (journalists) should be able to access (work with) TINFO at any location
- Developers should be able to develop, test and modify from any location
- TINFO should be accessed via web browser and HTTPS as well as HTML5 should be applied. The supported web browsers are:
  - Microsoft Edge
  - Google Chrome
  - Apple Safari
  - The following browsers will not be supported due to the reason of cost. Even if the browsers support HTML5, there are differences that need to be addressed in the code of the application for each browser. Testing of many browsers is time consuming and the security vulnerability is increased. Not recommended: Mozilla Firefox, Opera, Vivaldi, and other niche browsers on the market.

- Devices and OS that can be used (If budget allows apps can be developed, otherwise the scalability functions for browser can be implemented):
  - Desk- and laptops
  - Tablets
  - Smartphones
  - OS for device is of less importance as security which is built into the application and infrastructure, and selected OS should support web browsers above.
  - The solutions bring your own device (BYOD) as the security consideration is built into the application and infrastructure.
- GDPR requirements should be implemented in the functionality of TINFO and the organisation:
  - Lawful basis and transparency (design and go online)
  - Data security (design and development phase)
  - Accountability and governance – Loco News (design and go online)
  - Privacy rights (Design, development and go online)
- Requirements according to ISO 27002 should be implemented in the design of TINFO

The proposed system design can be deployed on own servers or as a cloud service. Deployment at own servers requires upgrade of all server-OS, change of the network architecture and perhaps some new hardware like firewall and a backup solution. The physical protection of servers must also be upgraded substantially with dedicated server room, security door, theft protection alarm, etc.

The selection between in-house servers or cloud-based servers is related to the capability of the corporate. Does Loco News have the competence to run the day-to-day servers by own resources or should it be outsourced to specialized third parties which is an important decision to consider. Our recommendation is that this new application should be developed on a cloud-based platform. Microsoft Azure or Amazon AWS are the two platforms that support all security needed for the application TINFO that are to be developed. Our recommendation is to choose Microsoft Azure platform, based on [11], [12]:

- Flexibility in server configurations and backup options
  - Ability of setting up production and development environment on separate servers.
- Built in programs for development of applications and extensive library with add-on possibilities for software to incorporate business intelligence, artificial intelligence and other type of plugins.
- Databases (modern and secured databases)
- Security functionality
  - Authentication and encryption keys in separate vaults
  - Threat protection
- Dynamic control of servers and auditing and monitoring of applications
- All current applications, file storage, image databases, etc. running on servers at Loco news can be easily migrated and transferred and deployed on Microsoft Azure platform and accessed as web services with all security functionality as for the TINFO application

4.1 Software design

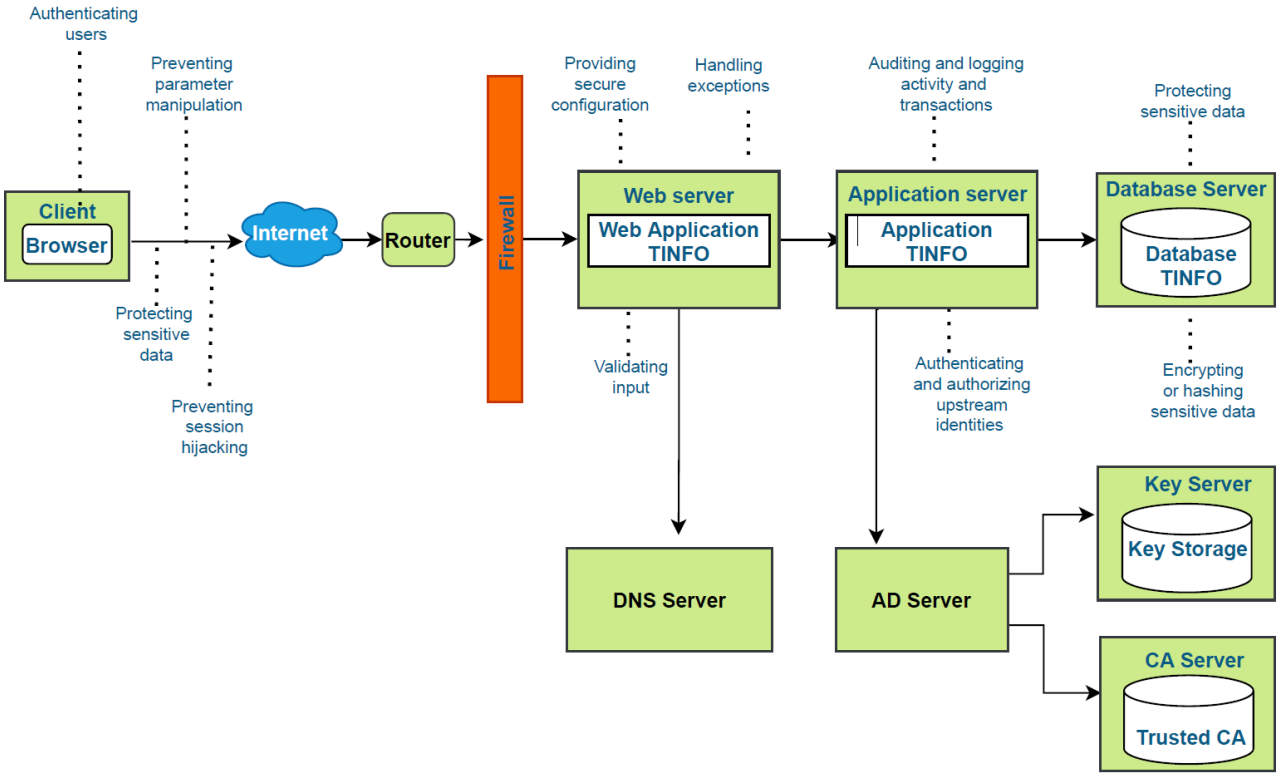

Figure5. The proposed software design for Loco News

Visual studio from Microsoft should be used to develop the TINFO application. The framework to use is the open source ASP.NET Core and the programming language to use is C#, which both are supported by Microsoft. The latest version of every individual package included in Visual studio for the ASP.NET Core framework should be used.

The users (clients) access the new application (TINFO) via the web browser (Microsoft Edge, Google Chrome or Safari) on the current devices (PC, Mac, Tablet, Smartphone). The OS on the client devices are of less importance as long as it supports one of the three browsers that the web application is programmed for. However, it is recommended that the OS on the devices upgrade to the latest version or a version that is still supported. It is good if the devices have programs that protect them from viruses. It is not mandatory as the security design of the TINFO-system has this type of protection.

TINFO has three layers and each layer runs on a dedicated server. Each server should have Windows Server 2016 as the operating system [13]. Windows Server 2016 supports all other software that should be used (ASP.NET, MSSQL) and the built-in webserver IIS should be used [14], [15]. The development of TINFO should be done in Microsoft Visual Studio 2019 [16], [17]. The programing language to be used is C# [18].

The open source framework ASP.NET Core should be used to program the TIFNO application [19]. The built-in tools and libraries in ASP.NET should be used [15]. For example, Razor and the Authentication system to be used when programming the TINFO web application. For secure storage

of encryption keys, the ProtectedData Class in the .NET framework should be used [20], [21]. The database is Microsoft SQL Server on all servers. Encryption of the database should be done using TDE (transparent data encryption) with an algorithm with 256-bit AES.

For the communication over the internet in the form of HTTPS the protocol TLS (transport layer security) version 1.3 or later should be used and no support for older versions of TLS or SSL (secure socket layer) are allowed. Cryptographic Hashing algorithms for certificates should be SHA-256. The SSL CA certificate should be bought from an authorized issuer like RapidSSL (https://www.rapidsslonline.com/).

All software above should be the latest available versions when the project starts and before TINFO going online. All the released patches and updates for the server OS and other software should be installed and tested.

4.2 Security Software design

There are four major software components to handle the security: First, the TINFO application with three layers. Each layer has coded functionality for security as well as using the other software described in this section. Second, specialized software to handle authentication in conjunction with authorization in TINFO. Third, there is software to handle keys for encryption and decryption of TINFO web applications and keys for encrypting and decrypting the databases. Fourth, there is software for auditing and monitoring of the TINFO application transactions.

Below is a description of the basic configuration for the security. Besides the above four major software components, there are also other important security software in the system like the firewall and intrusion prevention software described at the end of this section:

1. Input validation – involving as early as possible in the data flow. Not only ensuring the properly formed data is entering the workflow, but in the backend before the database is updated. Input validation should be programmed in each layer for TINFO application. The three basic types of validation are: data type validation, data format validation and data value validation. There is a whole lot more to input validation and injection prevention, however, the basic thing is that validation of inputs should be done with both a syntactical as well as a semantic approach. Syntactic validation should enforce correct syntax of information (SSN, birth date, currency or whole numbers) while semantic validation should enforce the correctness of their values within a very specific business context (end date is greater than the start date, low price is less than high price).
2. Encryption – the basic process of encoding information to protect it from unauthorized users to access it. Encryption should be applied to the web application layer and to the database using functions and keys in ASP.NET Core according to the previous section.
3. Authentication – when designing a web application, one very basic goal should be to give users as little privileges as possible for them to get what they need from the system. Using this principle of minimal privilege will vastly reduce the chance of an intruder performing operations that could crash the application or even the entire platform. In the web application authentication functionality to prevent browsers from storing passwords should be

implemented. Two-factor authentication using SMS to the focal mobile phone should also be implemented. Strong password is a double-edged sword. It makes it difficult to crack the password but the risk it that the user has a written note in his wallet or on the back of his phone and it becomes a very high security risk. Strong password should be setup like following rules: the password should contain characters, digits and special characters (e.g. "!", ",", "/", "#", "$", etc.) with a minimum length of 8 (e.g. "Cat1234=") which is defined in the AD (active directory) that contains the users of the system.

4. Authorization – should be conducted as an explicit check after authentication check when each time a function in TINFO makes a call to the databases. In the AD every user has an assigned role for TINFO. In the TINFO application the functionality for the authorization of each role is programmed. The role defines which information each role has access to and the rights for read, write, add or delete information in the databases for TINFO.
5. Configuration Management – Maintain computer systems, servers, and software in a desired, consistent state, including:
   a) All the components required for the application should be updated and the latest patches applied on them. The default configuration should be changed frequently.
   b) Sensitive Data: Sensitive data like database connection string, encryption key, admin credentials or any other secret should not be stored as plaintext in the code. The configuration file should be secured against the unauthorized access.
   c) Persistent cookies: storing sensitive data as plaintext in a persistent cookie should not be done as this allows the user to modify and see the contents.
   d) The GET protocol should not be used in the web application program since sensitive information can be accessed from the browser history or logs.
   e) Disable unused methods like TRACE, PUT, DELETE, etc. in the web application program and when applicable also for the application layer.
6. Session Management – A common vulnerability of web applications is caused by not protecting account credentials and session tokens. The user should automatically be logged out after 10 minutes of inactive. The built-in functionalities in Windows web server and ASP.NET Core should be used in the program which means that the default session management should be used.
7. Cryptography – All communication in the web interface is encrypted as well as the database. In the previous section the details of what should be applied in the program are specified.
8. Parameter Manipulation – All validation of data should be applied in the web application for TINFO. To ensure that no manipulation of data validation can be done in the browser (e.g. enter program code). Functions in ASP.NET Core to protect data should be set so data cannot be changed by entering code a manipulate date in the browser. Also see 6 above for setting the system parameters and functionality.
9. Exception Management – The application must have protocols to encounter unanticipated errors. The view (screen) for the user should never display anything more than just a

generic error message in case of a failure. When an error occurring, the transaction request made from the web application should always be rejected by the web application. This should be programmed in the web application.

10. Auditing and logging – Logging should be done for each layer of the application using the functionality built into the OS for the servers. Each layer is logged independently. There should also be applied logging in the firewall. The most important events to log from a security point of view is:
    a) The database, all editing, deletion and writes related to the tables. Fields that contain sensitivity in a table should also be logged.
    b) Input validation failures (e.g. protocol violations, unacceptable encodings, invalid parameter names and values)
    c) Output validation failures (e.g. database record set mismatch, invalid data encoding)
    d) Authentication successes and failures
    e) Authorization (access control) failures
    f) Session management failures (e.g. cookie session identification value modification)
    g) Application errors and system events (e.g. syntax and runtime errors, connectivity problems, performance issues, error messages from third party service, file system errors, file upload virus detection, configuration changes)

In conclusion, we design this software system based on a trade-off consideration, the balance between the safety of the system, the corporate's background, and the related efforts need to put in: The solution that TINFO can only be accessed from a PC connected ethernet cable to LAN (local area network) and the PC owning a key which is stored in the system. This will benefit the company-owned laptops when the journalists travel to work. But none of this is stronger than the weakest link in security. The basic security in our solution has to be applied in any case. Otherwise, if data is sent in plaintext and someone with the professional knowledge and equipment would be able to monitor the LAN or Wi-Fi which could lead to leakage of the sensitive information. If journalists suffer theft of the PCs, the proposed solutions will effectively hinder the criminals to access the sensitive information. Due to the application of multi-factor authentication, without authorization of the users' personal devices, it can be very challenge to access TINFO system.

The main reason for this solution is to enable a modern way of working for the journalists at Loco News which can be considered as a competitive edge. Latest news has to be reported in time, taking time to get to the office to write the article means giving the first chance to someone else in the news business. Other reasons include: it is a scalable solution that enable Loco News to grow. A new journalist can be hired as a "freelancer" who can use the system without having to work on-site. The system can create a user ID which can be sent by email and a one-time password will be sent via SMS. The new journalist can start to work immediately at the location where the news happened. The potential limitation of this system is that the user is the weakest link in security. The user itself could be the hacker to approach the "wanted information" of the system. However, the proposed design is able to effectively prevent the users without sufficient permissions to access the sensitive data of TINFO.

5. Use case scenarios

The new application to support business processes should be based on a modern and secure platform. Our solution will enable a modern way of working for the journalists at Loco News which will become a competitive edge to meet the present and future requirements. Based on the previous section, we now propose a brand-new system for Loco News to achieve the goals of the ability of adapting expand businesses as well as a better overall performance of information security. In this section, a series of case scenarios regarding the new system will be given in order to prove the reliability and safety of TINFO.

Table 1. Case scenarios in the workplace

Data management case scenarios in the workplace
Employee (user id) with assigned role and rights: view (information classified as Public or Company) **Activity:** search information in the server **System flow:** employee logs in the TINFO via the web browser. The user id and password are authenticated and the rights given to the user's session. The user searches through key terms such as date, name of the person, author, etc. To find information they may want to use as a base for a new article, the user can only view information that his role is authorized to view, according to the roles logic that is programmed in TINFO.
Employee (user id) with assigned role and rights: view all information and edit all Information **Activity:** add new information to an existing information record **System flow:** employee logs in the TINFO via the web browser. The user id and password are checked and the rights are applied to the user's session to edit or update existing information. The user finds the article he/she wants to add the new information to. Then the user clicks the edit button to make the view in the browser editable. User adds the new information and later clicks "save changes" then the employee proceeds to close the article or leaves the webpage. If the user closes the browser before they have clicked Save all then the document will be reverted to its previous state (see section 4.2).
Employee (user id) with assigned role and rights: view, edit, add and delete all types of information in the system. **Activity:** add a new article **System flow:** employee logs in the TINFO via the web browser. The user id and password are checked and the rights are applied to the user's session to edit or update existing information. The user selects the function "new article" in TINFO. The user starts with selecting "type of information" via a dropdown box. As the field "type of information" comes from another table in TINFO the dropdown box is populated with the values from that table. Some other mandatory fields are also entered. Finally, the user adds the information (articles) and selects "save". Then the input validation controls are activated. It will be validated if all mandatory fields are fulfilled in and that the format is correct. Some other validations will also be done in order to prevent that "hidden executable code" has been entered as information. When the system has validated the new record, it gets status "for approval" and a mail is sent to CEO Goran, so he can exercise his rights given by the policy we have made for Loco News. Goran reviews the article and marks the box "Checked" and the new record gets status approved and can be viewed by other users. If Goran does not approve the entered article he can click "declined" and enter a reason why the article is declined. A mail is sent to the user who reviews the article, saves it and it is once again sent to Goran for

approval. Only articles with status approved are viewed by the users. Article with status for approval can only be viewed by the user who has added the article and the one who set as approver for a new article.

The following cases describe how TINFO treats common errors made by personnel which are important for system security:

Table 2. TINFO reacting to common errors

Common cases
Case: Employee forgets to log off their TINFO account. **Solution:** The web application automatically logs out users after 10 minutes of in-activity.
Case: Employee tries to edit an article but his role does not have right to edit a record **Solution:** This will never happen as the button or menu function for edit is not viewed for this user.
Case: Goran does not approve all new articles so there is nothing to view in TINFO. **Solution:** Nothing to do about this common workflow error. Goran is the owner and does not take orders from any employee, security consultant or IT-system.

As the above mentioned, these are the major changes that may happen to the workplace after the implementation of TINFO. In addition to that, TINFO is also capable of defending against other forms of cyber-attacks. The suggested implementations will largely reduce the possibility of being influenced by viruses, malware, and other forms of internet threats as CTO stated. The new IT system will benefit Loco News' corporate competitiveness and business strategy.

References

[1] Tutorialspoint, "*Software Architecture & Design Introduction*", [2020-12-26], url: [https://www.tutorialspoint.com/software_architecture_design/introduction.htm]

[2] Standard Fusion, "*The Cost of a Failed ISO Audit*", [2020-12-26], url: [https://www.standard-fusion.com/blog/the-cost-of-a-failed-iso-audit/]

[3] Jnttek, "*No you cannot have Admin Access! (And why this is good IT policy)*", [2020-12-26], url: [https://www.jnttek.com/no-you-cannot-have-admin-access-and-why-this-is-good-it-policy/]

[4] Techopedia, "*Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)*", [2020-12-27], url: [https://www.techopedia.com/definition/22921/wi-fi-protected-access-pre-shared-key-wpa-psk]

[5] Agilites, "*Pros And Cons Of Using C# As Your Backend Programming Language*", [2021-01-08], url: [https://agilites.com/pros-and-cons-of-using-c-as-your-backend-programming-language.html]

[6] ISO and IEC, "*Information technology — Security techniques — Code of practice for information security controls*", [2021-01-06], url: [https://mymoodle.lnu.se/pluginfile.php/6312509/mod_resource/content/2/ISO_IEC_27002_2013.pdf]

[7] Studytonight, "*Components of DBMS (Database Management System)*", [2021-01-06], url: [https://www.studytonight.com/dbms/components-of-dbms.php]

[8] Blast, "*Data Management Consulting*", [2021-01-06], url: [https://www.blastanalytics.com/data-management]

[9] Arvind Singh Baghel, "*Software Design Principles DRY, KISS, YAGNI*", [2021-01-06], url: [https://www.c-sharpcorner.com/article/software-design-principles-dry-kiss-yagni/]

[10] Guru99, "*SQL Server Architecture Explained: Named Pipes, Optimizer, Buffer Manager*", [2021-01-08], url: [https://www.guru99.com/sql-server-architecture.html]

[11] Microsoft, "*Limitless data and analytics capabilities. Yes, limitless.*", [2021-01-08], url: [https://azure.microsoft.com/en-us/]

[12] Microsoft, "*Azure documentation*", [2021-01-08], url: [https://docs.microsoft.com/en-us/azure/?product=all]

[13] Microsoft, "*Windows Server*" [2021-01-08], url: [https://www.microsoft.com/en-us/windows-server]

[14] Microsoft, "*Windows Server Documentation*", [2021-01-08], url: [https://docs.microsoft.com/en-us/windows-server/]

[15] Microsoft, "*What is ASP.NET?*", [2021-01-09], url: [https://dotnet.microsoft.com/learn/aspnet/what-is-aspnet]

[16] Microsoft, "*Visual Studio 2019*", [2021-01-09], url: [https://visualstudio.microsoft.com/vs/]

[17] Microsoft, "*Visual Studio documentation*", [2021-01-09], url: [https://docs.microsoft.com/en-us/visualstudio/windows/?view=vs-2019]

[18] Microsoft, "*C# documentation*", [2021-01-09], url: [https://docs.microsoft.com/en-us/dotnet/csharp/]

[19] Microsoft, "*What is ASP.NET Core?*", [2021-01-09], url: [https://dotnet.microsoft.com/learn/aspnet/what-is-aspnet-core]

[20] Microsoft, "*What is .NET*", [2021-01-09], url: [https://dotnet.microsoft.com/learn/dotnet/what-is-dotnet]

[21] Microsoft, ".NET documentation", [2021-01-09], url: [https://docs.microsoft.com/en-us/dotnet/]