2022

A Trusted Platform for Unmanned Aerial Vehicle-Based Bridge Inspection Management System

Hwapyeong Song

A TRUSTED PLATFORM FOR UNMANNED AERIAL VEHICLE-BASED BRIDGE INSPECTION MANAGEMENT SYSTEM

A thesis submitted to
the Graduate College of
Marshall University
In partial fulfillment of
the requirements for the degree of
Master of Science
In
Cybersecurity
by
Hwapyeong Song
Approved by
Dr. Wook-Sung Yoo, Committee Chairperson
Dr. Paulus Wahjudi
Dr. Cong Pu

Marshall University
August 2022

APPROVAL OF THESIS

We, the faculty supervising the work of Hwapyeong Song, affirm that the thesis, *A Trusted Platform for Unmanned Aerial Vehicle-Based Bridge Inspection Management System*, meets the high academic standards for original scholarship and creative work established by the M.S. in Cybersecurity and the College of Engineering and Computer Sciences. This work also conforms to the editorial standards of our discipline and the Graduate College of Marshall University. With our signatures, we approve the manuscript for publication.

Dr. Wook-Sung Yoo, Department of Computer Sciences and Electrical Engineering
Committee Chairperson Date

Yoo, wook 07/08/2022

Dr. Paulus Wahjudi, Department of Computer Sciences and Electrical Engineering
Committee Member Date

Paulus Wahjudi 07/15/2022

Dr. Cong Pu, Department of Computer Sciences and Electrical Engineering
Committee Member Date

Cong Pu 07/13/2022

ACKNOWLEDGMENTS

This research would not have been possible without the support and encouragement of many people. I would like to express my first deepest gratitude to my advisor, Dr. Wook-Sung Yoo, who always remarkably made me enthusiastic about studying and learning. He has been the ultimate role model, giving thoughtful guidance and warm encouragement. He has provided diverse opportunities for me to grow professionally and has arranged astonishing experiences for me to broaden my perspectives. I am grateful for and proud of my time working with Dr. Yoo.

I am extremely grateful to Dr. Paulus Wahjudi, who made me feel enjoyable about my research through discussion. He has been an ideal mentor, providing advice and strong support with extraordinary insight and humor. Like he first proposed the creative name ‘iBIRD’, his constructive feedback helped a lot in expanding the idea from the very beginning of the research. It is an honor to learn from Dr. Wahjudi.

I am deeply indebted to Dr. Cong Pu, who guided me from the beginning of the thesis and enabled me to grow an understanding of the subject. He has been an amazing adviser, offering detailed feedback and assistance. He taught the course where I first implement lightweight mutual authentication for drones. Many of its concepts were applied with his help. I am fortunate to have worked with Dr. Pu on this thesis.

I am also thankful to Dr. Bob Hong for teaching me the basics of writing papers and for his guidance and academic support. I would like to extend my sincere thanks to Dr. Sanghoon Lee for his warm consideration and kind support. Many thanks to the professors who took me on as a student and continued to have faith in me over the years.

Lastly, I am extremely grateful for my parents and my sister whose unconditional love, constant support, and encouragement keep me motivated and confident.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Bridge inspection has a pivotal role in assuring the safety of critical structures constituting society. However, high cost, worker safety, and low objectivity of quality are classic problems in traditional visual inspection. Recent trends in bridge inspection have led to a proliferation of research utilizing Unmanned Aerial Vehicles (UAVs). This thesis proposes a Trusted Platform for Bridge Inspection Management System (Trusted-BIMS) for safe and efficient bridge inspection by proving the UAV-based inspection process and improving the prototype of the previous study. Designed based on a Zero-Trust (ZT) strategy, Trusted-BIMS consist of (1) a database-driven web framework with security features for bridge inspection management, (2) a mobile interface supporting the inspection data collection using UAVs, and (3) a mutual authentication protocol for the Internet of Things (IoTs). The server script language used to implement the web system was PHP and React Native was used for the mobile application development. The secure communication algorithm used server-side PHP and client-side JavaScript, and MySQL was adopted as the database. This paper provides an overview and details of Trusted-BIMS and demonstrates the overall process of bridge inspection using UAVs and applied technologies to the proposed platform. The result of this research will make an important contribution to the field of UAV-based bridge inspection. Further research can be conducted on refined implementations of security algorithms, more comprehensive security schemes, and machine learning technology to reduce human intervention.

Keywords: unmanned aerial vehicle; bridge inspection; software development; cybersecurity; zero-trust; mutual authentication

CHAPTER 1: INTRODUCTION

1.1 Background

Bridges are one of the most important infrastructures in contemporary civilization and bridge inspections are vital components in guaranteeing the safety of the key architectures constituting society. Biennial bridge safety inspections are mandated by law to increase safety as well as the longevity of these vital infrastructure components. Although the mandated inspections must be conducted by state-certified inspectors who are required to fill out inspection forms, creating a database of bridges and setting priorities are not required by law. The traditional visual inspection has accessibility limitations, high cost, and safety risks. To solve these issues, some states have begun to explore the use of rapidly growing UAV technology, resulting in cost savings of three-fifths over manual inspection (Lovelace & Wells, 2018b; Lovelace & Zink, 2015; Zink, 2016). Some capstone project teams at Marshall University recently created a prototype of the interactive Bridge Inspection Research using Drone (iBIRD) as proof of the concept (Song et al., 2022).

In an attempt to further develop the prototype, this research project is to implement an intuitive web framework used for bridge inspections with secure communication among UAV, Cloud, and computer devices and to improve the quality of the mobile application. The system consists of (1) a database-driven web application of the Bridge Inspection Management tool, (2) a mobile application gathering inspection data from UAV, and (3) an application of a lightweight authentication system designed for the IoT devices used in the bridge inspection process.

1.2 Problem Statement

Bridge inspection is important, but the mandated inspections conducted by state-certified inspectors can be expensive and have several issues. It is necessary to control traffic during inspections and to use a variety of equipment to check the bridge components, including under-bridge inspection vehicles and lifts. It is these factors that increase the costs of inspection. Besides, the issues related to costs frequently delay periodic close-up inspections of bridges in some large cities (Lovelace & Wells, 2018b). There are over 7,314 bridges in West Virginia alone (U.S. Department of Transportation Federal Highway Administration, 2021) and the United States allocates approximately $15.6 billion per year for the maintenance of the infrastructure (Kirk & Mallett, 2018). Most inspections are conducted visually by state-licensed inspectors. Whereas a small-sized bridge may only need an inspector using a small ladder, other larger bridges that require more detailed under-bridge inspections may require a truck unit with a bucket attachment so the inspector can be lowered under the bridge for a detailed investigation (Leonard, 2015). Bridge inspection teams first visually inspect a bridge looking for signs of rust and weakened joints, and they examine the supports holding up the bridge. If the visual examinations indicate a problem, more detailed inspections are conducted, which include the use of an X-ray device that examines for hidden cracks or fatigue (Madden, 1983). Most bridges are, therefore, only visually inspected but the current visual inspection process still suffers from high costs and operator safety issues. These issues can be traced to the underlying problems arising from manual inspections.

First, one such issue is the high expenditure of the federal, state, and local transportation agencies on annual bridge inspections. With the aging of bridges, the number of structures requiring bridge maintenance work increases. This is one of the reasons that the inspection cycles are shortened. As a result, it is predicted that higher costs will be required, including budget allocations for work time and worker training.

Second, visual inspections are conducted in such a way that the operator directly observes the bridge. Since bridges are usually installed at high altitudes from the ground, there is a risk of falling, and inspections are limited to locations that are inaccessible to humans. Inspections are also greatly affected by the skill level of the operator.

Third, according to the background research conducted, there are limited studies related to systems that display and manage bridge inspection data in a meaningful way. Although data are collected annually for reporting purposes, suitable web applications that can keep track of the data have not yet been developed. For such an application to be implemented, besides a well-structured database that plays an important role in its implementation, proper classification and storage of data are essential. In addition, various skill levels of the operator that affect the quality of the inspection further necessitate the development of a platform that can share and integrate information between working parties.

Fourth, with the use of UAVs, the protection, transmission, and storage of the data acquired during the inspection process is a notable issue. According to the Cybersecurity and Infrastructure Security Agency (CISA), bridges are one of the critical infrastructures in society, and the disabling or destruction of these infrastructures is considerable implications for national security, the economy, and public health (Cybersecurity and Infrastructure Security Agency CISA, 2020). Inspections make it possible to identify and check the weaknesses of bridges, and this information has the potential to be used or might be used by malicious attackers to disable or destruct critical architectures. It means that sensitive data is handled throughout the entire process of the inspections. Data captured by unauthorized users can be a threat to the infrastructure.

Based on the issues identified above through research, the following two ideas are suggested to be considered at the level of the State Department of Transportation to solve problems arising from manual inspections:

1) a new method of inspection that can replace the traditional inspection method and

2) a safe framework to effectively display and manage inspection data.

1.3 Objectives

The objectives of this research project are to design and implement a Trusted Platform for Bridge Inspection Management System (Trusted-BIMS) to conduct safe and cost-effective bridge inspection using UAVs and to provide a secure streamlined bridge inspection and reporting process. The system will consist of (1) a database-driven Bridge Inspection Management web application with security features; (2) a mobile app gathering inspection data from UAV; and (3) a secure communication protocol for the IoT. Moreover, this study will provide a provision of user-friendly web applications with not only data drill-down functions but also security features, introducing zero-trust architectures to establish a trusted platform.

1.4 Contributions

This research has the following contributions:

1) Presenting a comprehensive review of the UAV-assisted bridge inspection process.
2) Developing and demonstrating an intuitive web framework and mobile application for bridge inspection.

3) Reviewing the security vulnerabilities of IoT devices used for bridge inspection and proposing an appropriate security scheme.

The results of this study will be of value to federal, state, and local transportation agencies and industry practitioners conducting bridge inspections.

1.5 Organization

The primary methods of conducting this research are web framework development, cross-platform mobile application implementation, and security schema modeling for IoT devices. To investigate the effectiveness of UAV-based bridge inspection compared to manual bridge inspection, academic research on industrial practices and implementation methods of bridge inspection using UAVs was performed for the first step. Chapter 2 includes literary reviews of traditional manual bridge inspections, UAV-based bridge inspections, UAV regulations, and cybersecurity issues related to platforms and entities for bridge inspection. In this study, how drone technology can be applied to bridge inspections will be researched, and related studies of other State Departments of Transportation will be reviewed. As a basis for implementing a trusted platform, this study will also be conducted on potential vulnerabilities that may arise from the use of UAVs, and on secure communication protocols, especially lightweight protocols.

Based on the basic research, a web platform and a mobile application for UAV-based bridge inspection are implemented. For secure communication, a Physical Unclonable Function (PUF)-based authentication algorithm is applied to the system and simulated. Chapter 3 presents the overview of the proposed schema consisting of these three modules, Trusted-BIMS. This chapter includes descriptions of each module as well as the overall UAV-based bridge inspection process. Chapter 4 details the design of Trusted-BIMS. In this chapter, a specification of each system is provided. The major functions implemented in each module and submodule are also described with figures. In Chapter 5, the security and threats to the proposed schema are analyzed based on the ZT model. Chapter 6 describes the findings and significance of this research. Finally, Chapter 7 concludes this thesis with a conclusion and future research. This thesis explains the overall framework of research on a trusted platform with built-in security features for UAV-assisted bridge inspections based on a comprehensive review and understanding.

CHAPTER 2: LITERATURE REVIEW

2.1 Manual Bridge Inspection

Manual bridge inspection is a method in which inspectors directly go to the site and visually inspect the bridge. Because of this characteristic, it is called visual bridge inspection. West Virginia is taking this approach, therefore, in this thesis, this method is also referred to as traditional bridge inspection.

The literature review shows that there are several issues with manual inspections. This traditional visual method has accessibility limitations, high cost, and worker safety risks. First, visual inspections are usually expensive compared to other methods. The experience and knowledge of the officials play a significant role in the manual inspection. It is also necessary to control traffic during inspections and to use a variety of equipment to check the bridge components, including under-bridge inspection vehicles and lifts. It is these factors that increase the costs of inspection. The Michigan Department of Transportation (MDOT)'s estimate that traditional inspections cost about 3.8 times more than drone inspections supports this fact (The American Association of State Highway and Transportation Officials (AASHTO), 2019). Besides, in some large cities, cost issues frequently cause delays in routine close-up bridge inspections (Lovelace & Wells, 2018b). Second, safety is one of the major issues. The safety of the officials and the traveling public continues to be jeopardized by visual inspections. This method often requires work in areas that are difficult to access by humans. There is also a risk of failure of access equipment. Lane closures are a significant contributor to the risk of injury and death (Lovelace & Wells, 2018b). Third, the collection method of manual inspection limits the effective management of data. In the traditional way, officials directly sketch, photograph the bridge, or hand-write relevant content at the collection site (Leshko, 2015). Digital devices are then used to create electronic documents. Depending on the skill of the inspector, there might be significant differences in the result of inspections because they are prone to subjective evaluations and assessments. It means that critical defects in the bridge may not be uncovered for a long time depending on the inspectors due to no platform to guide the inspectors and share data between working parties. In response to these problems, the need for effective data management and improvement of reporting process has emerged. However, there currently is limited research on tools that can adequately manage inspection data and reports. To my knowledge, there is no notable solution that can manage longitudinal data, and the software distributed to the relevant officials has some discrepancies from the actual inspection report content. Although some Departments of Transportation conduct research using 3-dimensional models, they use software dedicated to mapping (Lovelace & Wells, 2018a) and are not integrated with the report creation process. Monitoring bridge conditions to apply timely preservation activities to keep "good bridges good" and prevent more bridges from being classified as deficient is a goal every municipality should embrace. However, limited progress has been made in managing data collected by inspection to provide cost-effective decision-making (Leonard, 2015) but no comprehensive reporting system exists.

From a security point of view, confidentiality related to the disclosure of bridge inspection reports is one of the most frequently stated issues with traditional bridge inspections. The Department of Homeland Security (DHS) is concerned about the disclosure of information on critical infrastructure, arguing that exposure to vulnerabilities in such infrastructure could be a potential threat utilized for attack by malicious users (U.S. Department of Homeland Security, 2009). For this reason, the Pennsylvania Department of Transportation (PennDOT) treats the bridge inspection information as confidential and does not disclose it to the public (Pennsylvania

Department of Transportation, 2021). This suggests the need for limited access control by restricting access to the full due diligence report. Moreover, in the case of disclosing some transportation maintenance activity data for the public's right to know, suitable data classification regulations are required, such as excluding sensitive information that can incapacitate infrastructure. Several West Virginia bridge inspection reports are accessible through a web search engine, Google. This means anyone can download the data. To ensure confidentiality and adequate access control, a new platform that provides access only to authorized entities is required.

Maintaining integrity has been the subject of considerable discussion. Traditional bridge inspections perform the process of converting field investigation data into digital reports. In other words, the contents of the notes made on-site are converted into digital form by inspectors. In this process, time gaps and spatial differences arise. This can make it difficult to tightly control entities and resources to maintain integrity. Data may be changed in the process of converting handwriting, and this may reduce the accuracy of the data. It is also difficult to prove that only authorized users have access to the resource. The characteristic of this process is also closely related to the availability of data. If the note or camera recording the inspection is lost, the data is also lost and cannot be recovered. This raises the need for a framework that can directly transmit data from the field to remote locations.

According to literature analysis of manual bridge inspection, the research to date has tended to focus on the inspection process itself rather than security. This, therefore, indicates that research on a platform and process that can resolve the security issues of the traditional method while presenting a new cost-effective schema needs to be conducted.

2.2 UAV-based Bridge Inspection

Bridge inspection using UAVs has been proposed to replace the traditional inspection method. UAV-based bridge inspection refers to the use of UAVs in the bridge inspection process. In other words, instead of inspectors directly approaching the bridge and taking pictures, the UAV carries out this work. In the United States, some states explore the use of rapidly growing UAV technology as summarized in Table 1.

Applied or tested UAVs for bridge inspection	***Researching the potential use of UAVs***
Alabama	Minnesota
Alaska	Florida
California	Idaho
Colorado	Iowa
Connecticut	Kansas
Georgia	Louisiana
Kentucky	Michigan
Maine	New York
Nevada	South Carolina
New Jersey	South Dakota
North Carolina	Vermont
Ohio	Wisconsin
Oregon	
Utah	

Table 1: List of states that have applied or are researching bridge inspection using UAVs

Fourteen states, including California, have introduced UAV-based bridge inspection, and 12 states, including Minnesota, are actively researching the potential use of UAVs (The Western Transportation Knowledge Network (WTKN), 2018; United States Department of Transportation, Bureau of Transportation Statistics, 2022; Seo et al., 2018; Georgia Department of Transportation, 2019; ROAD&BRIDGES, 2016; ROADS&BRIDGES, 2020; ROAD&BRIDGES, 2021; Burgett et al., 2019; NJDOT Bureau of Research, 2022; Federal Highway Administration, 2021). The Minnesota Department of Transportation has completed a third phase of research focused on utilizing drones as a tool to improve the quality of bridge inspections in 2019, reported an average cost saving of 40%, and showed a dramatic reduction in risks for the public and transportation workers (Lovelace & Wells, 2018b).

2.3 UAV Regulations

To protect civil privacy and maintain social order, the use of UAVs is regulated by law. This means there are legal limits on the use of UAVs for bridge inspection. According to the Federal Aviation Administration (FAA), drones used for commercial purposes must meet the requirements of Title 14 Code of Federal Regulations (CFR) Part 107 (Federal Aviation Administration, 2021b). The regulation includes the requirement that FAA certification of UAV pilots through testing is required, as well as the provision to register drones every three years. State officials should operate UAVs under Part 107 rules or should obtain an FAA certificate of authorization (COA) (Federal Aviation Administration, 2021e). The use of drones for research purposes is governed by the Recreational Flyers Rule by 49 USC 44809 and Public Law 115-254 Section 305 (Federal Aviation Administration, 2021c). In this case, UAV registration is not required if the Aircraft weighs less than 250g (Federal Aviation Administration, 2021d), but a certificate of passing The Recreational UAS Safety Test (TRUST) is required (Federal Aviation Administration, 2022). The flight area also is limited due to safety issues. The FAA classifies airspace into A-E and G classes in consideration of the surrounding infrastructure, and flight conditions vary according to these classes. Figure 1 shows the flight regulation by class (Federal Aviation Administration, 2021a).

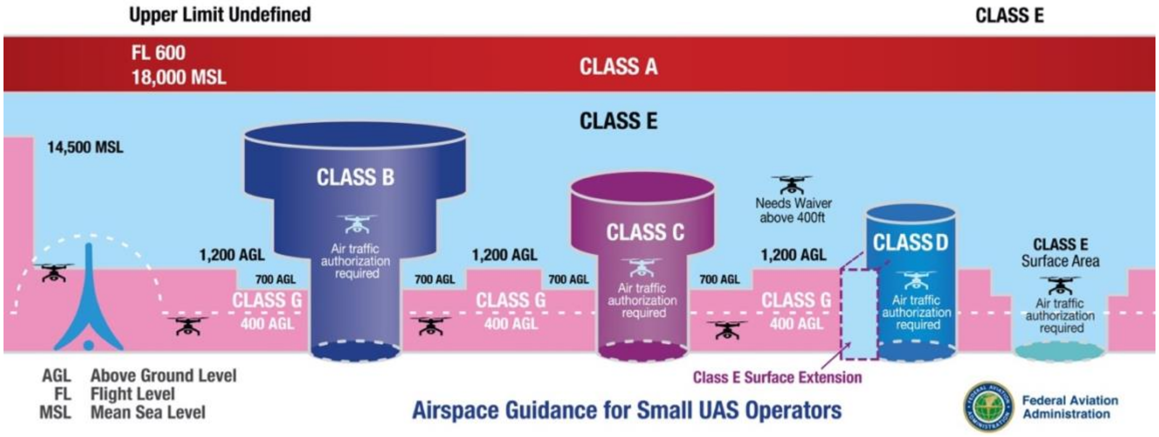
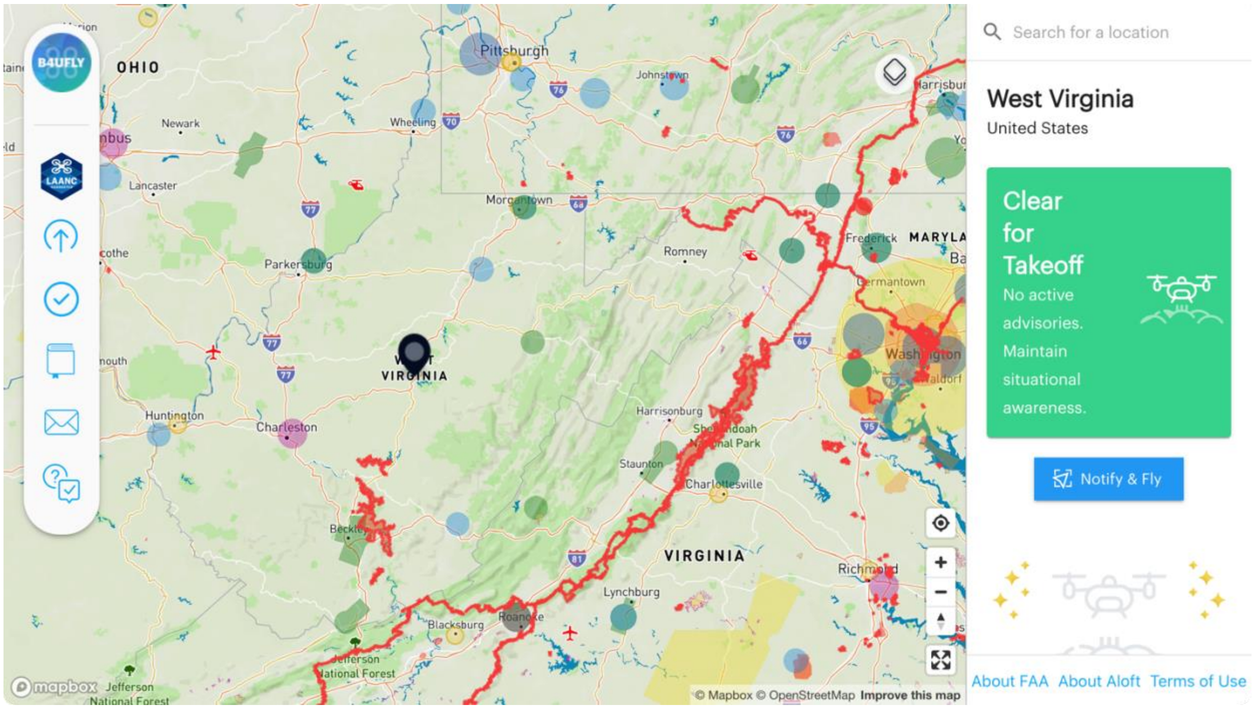


Figure 1. Flight Regulation by Class (Federal Aviation Administration, 2021a)

Flights are generally permitted within Class G airspaces, and flight altitudes are limited to within 400 feet from structures. Other classes of airspace require additional FAA permits to fly UAVs. Therefore, pilots should check the class and regulations of the area before flying the drone. Figure 2 shows airspace regulations in West Virginia and around the area (Aloft, n.d.).



Search for a location

West Virginia
United States

Clear for Takeoff
No active advisories. Maintain situational awareness.

Notify & Fly

About FAA About Aloft Terms of Use

Figure 2. Airspace Regulations in West Virginia (Aloft, n.d.)

2.4 Cybersecurity

Cybersecurity Basics

Developing a trusted platform requires a certain level of cybersecurity. According to the Committee on National Security Systems (CNSS, 2015), cybersecurity is a comprehensive concept that refers to the protection and defense of systems to ensure five characteristics: confidentiality, integrity, availability, authentication, and non-repudiation.

Confidentiality is the disclosure of information only to authorized users (CNSS, 2015). The word ‘user’ in this context means every entity, including individuals, software, and hardware (United States Naval Academy, n.d.). Confidentiality is important to ensure personal privacy and to prevent sensitive information such as personal information and business ideas from being stolen or misused. This property can be ensured by restricting users’ authority and access, encrypting data, etc.

Integrity is that information is not altered in an unauthorized way (Ross et al., 2016). This is a principle that should be followed to ensure the consistency of information, the accuracy of resources, and the completeness of data (United States Naval Academy, n.d.). In other words, maintaining integrity is an important factor in increasing the reliability of the system. This can be realized through the validation of data or files using hash functions.

Availability allows authorized users to have reliable access to information and systems (CNSS, 2015). Providing timely data is one of the fundamental reasons information systems exist. Availability can be ensured by devising countermeasures to prevent, protect, and respond to physical threats such as theft and loss of physical medium and attack defense that disable the system by controlling access to the system.

Authentication is the verification of the eligibility of an entity, which may be required in a variety of situations, including user access to the system, and sending messages (CNSS, 2015). This is essential to secure systems and build a reliable platform. If authentication is not performed, information may be leaked or used with malicious intent by unauthorized entities, and the system may be altered or destroyed. Authentication can be provided through the introduction of a secure authentication algorithm.

Non-repudiation means protecting against denying certain activities (National Institute of Standards and Technology, 2020). Examples of such actions are information system access or data processing. This property improves the reliability of information and systems and helps maintain their integrity. If Non-repudiation is not guaranteed, there is a possibility of undermining the user's accountability. To ensure this property, user activity logs may be recorded and archived, and a method of identifying the user using a digital signature can be applied to the system.

Cybersecurity on UAV-based bridge inspection

Although bridge inspection using UAVs provide multiple benefits, it will expose the system to several cybersecurity challenges, like any other communication device. Representatively, there are man-in-the-middle attacks, which manipulate network communication to eavesdrop or manipulate communication contents, and Known Session Key attacks, which use outdated session keys to gain unauthorized access. Stolen smart device attacks, which physically steal the device, are also major issues. Using the diverse attack methods, attackers can steal the UAV and IoT device controlling the UAV or the information the IoT has.

Due to the vulnerabilities, CISA has proposed to encrypt both stored and in-transit data in operations with UAVs to ensure confidentiality and integrity (Cybersecurity and Infrastructure Security Agency CISA, 2019). To provide secure data transmission between UAV and IoT devices and clouds, considerable research has been conducted. UAVs and IoT devices are limited in power, process, and memory. These features make it difficult to apply traditional cryptographic protocols. Most of the research in the field of portable device security systems, therefore, focuses on lightweight encryption system approaches.

One example is the design of a lightweight authentication system between entities involving UAVs. Some studies used encryption based on user identity (Zhang et al., 2020). The control server grants an identity-based private key to the UAV and users during the pre-registration process. Using the given private key, the drone and the users perform mutual authentication and access the server. In this authentication method, the process of obtaining the private key in advance must be preceded, and it is not suitable for real-time applications.

Another study presented a digital signature-based lightweight protocol between UAV and ground station, which was effective in defending against man-in-the-middle attacks and showed better performance in terms of cost, such as energy consumption and computation time (Li & Pu, 2020). In a similar study, a protocol for securely collecting and storing data through mutual authentication between two entities was presented, and it was demonstrated that communication overhead and computational cost were low and that the proposed mechanism provided better security (Pu et al., 2022).

In recent years, there has been an increasing amount of literature on authentication systems based on physical clone protection was studied. The PUF-based mutual authentication method generates encrypted messages using the identity of the IoT device and the unique physical fingerprint of the machine (Aman et al., 2017). Because a new set of challenges and responses are created each time authentication is performed, even if an attacker obtains the session key, the password set by the server cannot be inferred. In another major study, the lightweight protocol for mutual authentication between UAV and ground station, which introduced the PUF concept, showed better performance in computational cost and communication overhead compared to the existing encryption technology (Pu & Li, 2020). This concept has proven that it can respond well to widely known security attacks (Pu et al., 2022).

Based on this review, PUF-based authentication will be simulated as a security function to provide secure transmission of inspection data from an IoT device to an inspector's computer device and a cloud, ensuring security and countermeasures for potential vulnerabilities in IoT devices used throughout the proposed inspection process.

CHAPTER 3: OVERVIEW OF TRUSTED-BIMS

Trusted-BIMS is designed to support bridge inspection using UAVs. This schema is involved in all inspection phases such as assigning work, conducting site inspections, generating reports, and analyzing inspection data. Figure 3 shows the high-level system diagram of the proposed system.

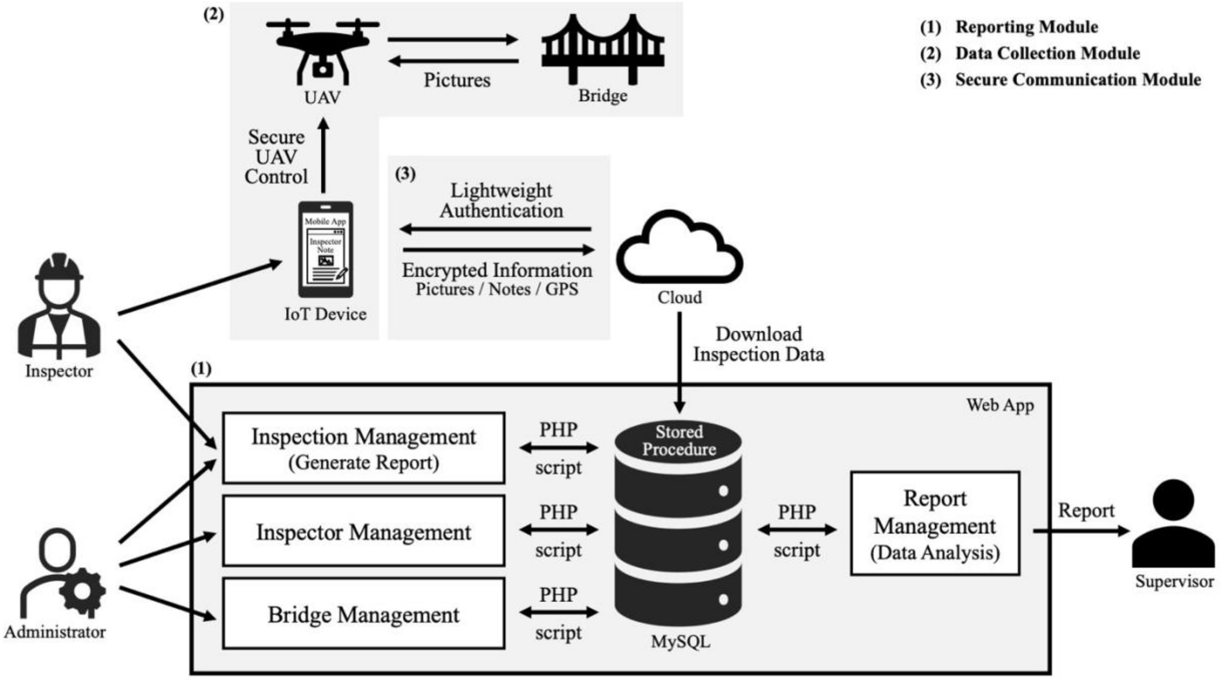


Figure 3. The Proposed High-Level Diagram of the Framework

This system consists of (1) a secure database-driven web application of the Bridge Inspection Management tool, (2) a mobile app gathering inspection data from UAV, and (3) an application of a lightweight authentication system designed for IoT devices used in the bridge inspection process. The overall framework of UAV-based bridge inspection research with built-in security features is described based on a comprehensive review and understanding.

3.1 Reporting Module

The reporting module uses the data collected by the UAV to describe the overall process for the inspector to create bridge inspection reports via a web application. As part of this module, a bridge inspection management system will be developed using PHP. The web system includes four main features: Inspection Management, Inspector Management, Bridge Management, and Report Management.

The entities that make up the reporting module are inspectors, administrators, supervisors, client devices, and data servers. Among them, the human entity is closely related to the role of the worker, and they access the web application using the client device, like a desktop. In this module, the web framework is implemented based on communication between the client device and the database server and provides functions necessary for the human entity's bridge inspection process.

Inspectors utilize the program to create inspection reports based on the data collected. The inspection management submodule supports the entire process from inspection assignment to generating inspection reports. Administrators assign inspections to workers, review the created inspection reports, add users with inspector privileges to the system, and manage overall information about the bridge, including bridge elements. The web application supports these tasks by providing inspection, inspector, and bridge management submodules. Supervisors require data analysis on the state-wide bridge inspection status by year and the risk of bridges. The report management submodule provides the drill-down functions for analysis. The client device provides an interface to human entities and acts as a bridge to connect with the database server. The data server stores the data used in the whole bridge inspection process and provides the data users need. In this way, the entities constituting the reporting module are organically connected.

By utilizing the reporting module developed on this platform, the overall bridge inspection can be managed, from the inspection assignments to report generating. This module makes a major contribution to research on UAV-based bridge inspection by demonstrating the process of utilizing 3D models of a bridge created using a UAV in the writing reports. Officials can intuitively understand the bridge state through this 3D model. In addition, this module supports easy report creation by making the data collected by inspectors accessible from the web interface. Besides, it is meaningful in that it not only displays and manages the bridge inspection data collected annually in a meaningful way but also archives it so that the data can be traced over a long period of time. The implementation of this module provides a platform to share information between different stakeholders.

3.2 Data Collection Module

The data collection module covers the process by which inspectors use IoT devices and UAVs to obtain information about bridges and bridge elements. It also includes simple APIs for transmitting data directly from an IoT device to a remote database. The entities that make up the data collection module are inspectors, UAVs, IoT devices, and a data server. Inspectors communicate with the UAV via an IoT device and send the collected data to a server via a mobile application. UAVs take pictures of bridges and are used to collect fundamental data for 3D models, GPS information, inspection data, etc. IoT devices provide the inspector with an interface to use the mobile unit and temporarily store the information collected from the UAV. A data server stores the information transmitted from the IoT device and provides the data to be used for inspection reports in the web framework.

The data collection module allows inspectors for rapid collection and ensures the inspection data is available as soon as possible. In addition, this module provides the function to send the collected data from the field to the data center, preventing data loss due to physical threats such as loss of inspection notes.

3.3 Secure Communication Module

A secure communication module is closely related to the data collection module. This security module is for the user and device authentication when sending the data collected and organized by the inspector to the server. In detail, a secure schema and mobile application are designed for secure data exchange between IoT devices and the cloud server. The entities that make up this security module are IoT devices and a server. These two entities have a form of two-way communication that sends and receives encrypted messages and codes that authenticate the messages, using the fingerprint of the IoT device. Each entity performs mutual authentication by verifying exchanged information using the unclonable unique value of the IoT device.

The secure communication module authenticates users and devices, making it difficult for unauthorized entities to alter the contents of the data server. This authentication feature ensures that data integrity is maintained, but also guarantees the reliability of the data transmitted by the authenticated device. It is, therefore, designed to prevent unauthorized database access and attacks using garbage data insertion. It also protects the server from being compromised by unauthorized users.

CHAPTER 4: SYSTEM DESIGN

Before describing the implementation, the bridge information and all of the inspection data presented in this thesis are mock data created for demonstration purposes only, and it is not actual data. All figures do not reflect real inspection and the data used in this paper do not imply that actual bridges are dangerous.

4.1 Web Framework

To provide bridge inspections using UAVs, a web application that interacts with the objects was developed. This application uses PHP as a server-side scripting language and has been tested using MAMP and XAMPP, a local server environment. It also has been tested using HostGator, a remote hosting server. This system uses a MySQL database to store data. MariaDB server was used as the database management system. The proposed web schema uses stored procedures to provide better security by avoiding displaying the SQL in plaintext on the client-side. More detailed information on the applied stored procedures can be found in *Appendix C*. Figure 4 shows the data flow of the implemented web system.

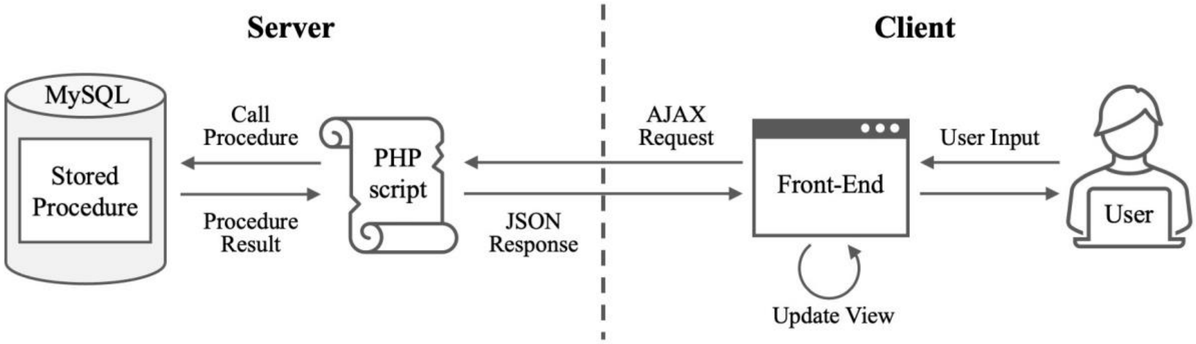
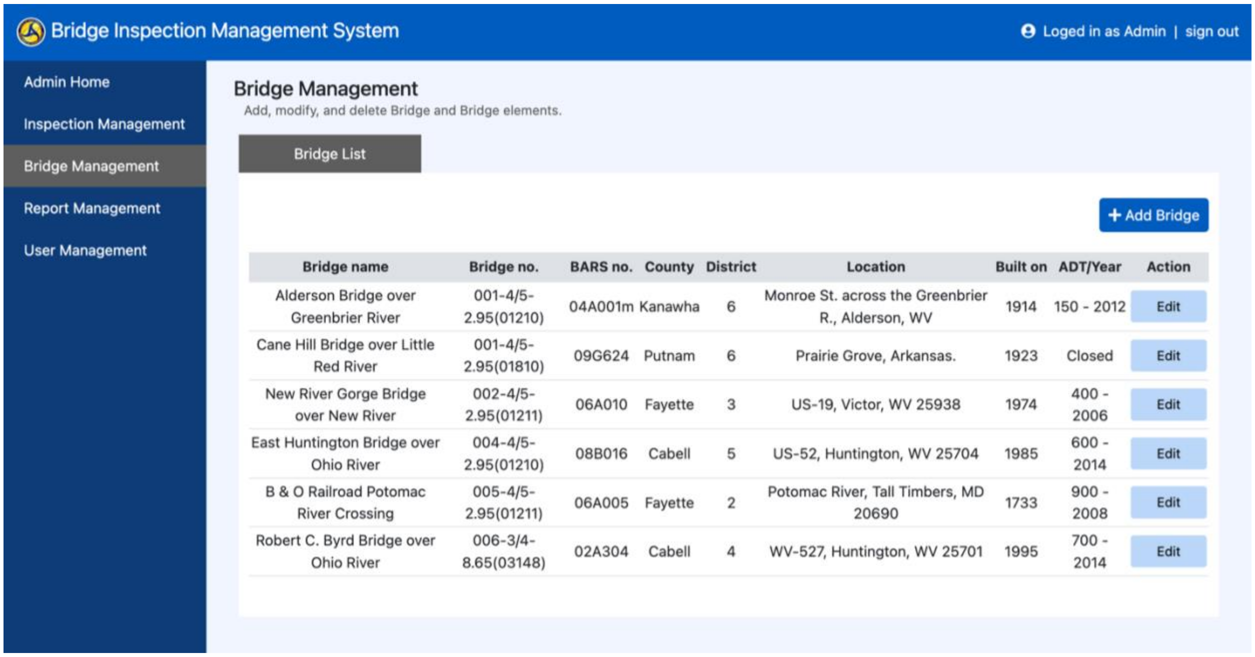


Figure. 4. Data Flow Diagram

Bridge Management

Bridge management enables integrated management of the overall information of bridges. Figure 5 shows the main page of the bridge management. Using this, administrators can add, remove, and update bridge data. This data includes basic information such as bridge name, location, and built year, as well as bridge numbers and Bridge Analysis and Rating Systems (BARS) numbers required for administrative management. Furthermore, a 3D model of the bridges with the marked important bridge components to examine is included. Notably, this modeling data help inspectors decide which elements of the bridge need to be inspected.

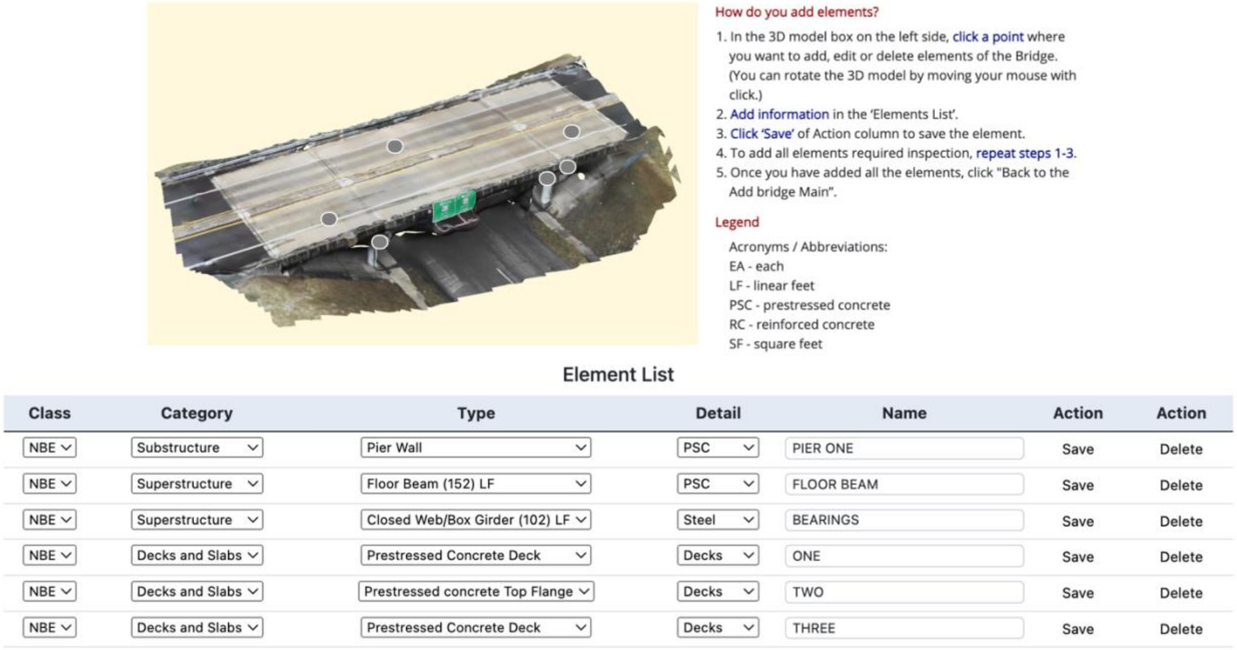


Bridge Management

Add, modify, and delete Bridge and Bridge elements.

Bridge name	Bridge no.	BARS no.	County	District	Location	Built on	ADT/Year	Action
Alderson Bridge over Greenbrier River	001-4/5-2.95(01210)	04A001m	Kanawha	6	Monroe St. across the Greenbrier R., Alderson, WV	1914	150 - 2012	Edit
Cane Hill Bridge over Little Red River	001-4/5-2.95(01810)	09G624	Putnam	6	Prairie Grove, Arkansas.	1923	Closed	Edit
New River Gorge Bridge over New River	002-4/5-2.95(01211)	06A010	Fayette	3	US-19, Victor, WV 25938	1974	400 - 2006	Edit
East Huntington Bridge over Ohio River	004-4/5-2.95(01210)	08B016	Cabell	5	US-52, Huntington, WV 25704	1985	600 - 2014	Edit
B & O Railroad Potomac River Crossing	005-4/5-2.95(01211)	06A005	Fayette	2	Potomac River, Tall Timbers, MD 20690	1733	900 - 2008	Edit
Robert C. Byrd Bridge over Ohio River	006-3/4-8.65(03148)	02A304	Cabell	4	WV-527, Huntington, WV 25701	1995	700 - 2014	Edit

Figure 5. Bridge Management on the administrator’s side



How do you add elements?

1. In the 3D model box on the left side, click a point where you want to add, edit or delete elements of the Bridge. (You can rotate the 3D model by moving your mouse with click.)
2. Add information in the 'Elements List'.
3. Click 'Save' of Action column to save the element.
4. To add all elements required inspection, repeat steps 1-3.
5. Once you have added all the elements, click "Back to the Add bridge Main".

Legend

Acronyms / Abbreviations:
EA - each
LF - linear feet
PSC - prestressed concrete
RC - reinforced concrete
SF - square feet

Element List

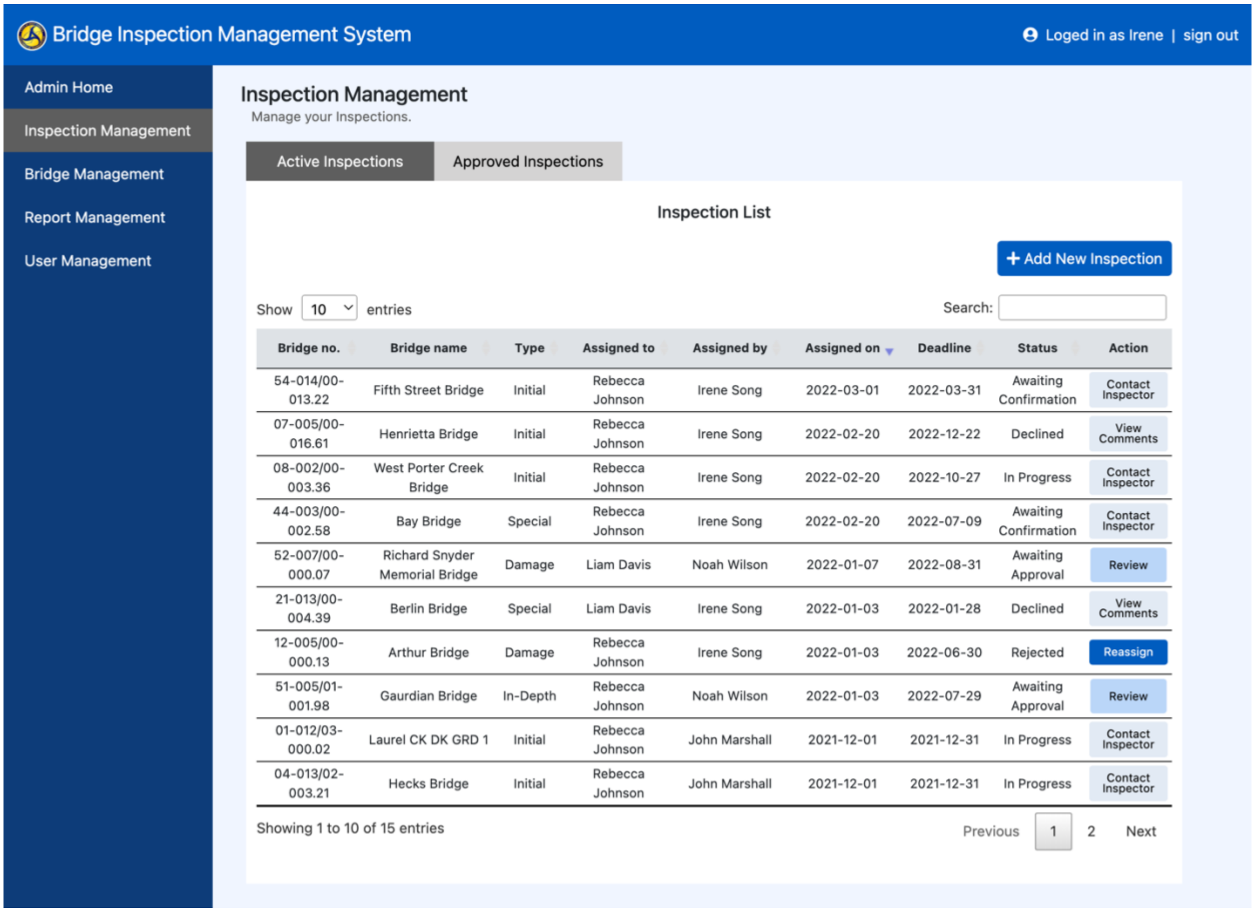
Class	Category	Type	Detail	Name	Action	Action
NBE	Substructure	Pier Wall	PSC	PIER ONE	Save	Delete
NBE	Superstructure	Floor Beam (152) LF	PSC	FLOOR BEAM	Save	Delete
NBE	Superstructure	Closed Web/Box Girder (102) LF	Steel	BEARINGS	Save	Delete
NBE	Decks and Slabs	Prestressed Concrete Deck	Decks	ONE	Save	Delete
NBE	Decks and Slabs	Prestressed concrete Top Flange	Decks	TWO	Save	Delete
NBE	Decks and Slabs	Prestressed Concrete Deck	Decks	THREE	Save	Delete

Figure 6. A 3D model with marked bridge elements

As shown in Figure 6, bridge elements and their details are included in the 3D model. Administrators can manage bridge elements that require inspection. Those elements are displayed as gray dots in the model. After conducting on-site inspections, inspectors can rate the risk on a scale of 1 to 9 for each bridge element. Depending on the rate, the elements at each inspection can be marked in different colors. This feature provides visual identification of the elements that require further actions. It also gives a detailed picture of the condition of the target bridge.

Inspection Management

Inspection Management plays an important role in the entire inspection process, including assignment and execution of inspections and report generating. As seen in Figure 7, administrators can assign five types of inspections: Initial, Routine, In-Depth, Damage, and Special. The inspection status can be monitored from this inspection list, the types of which are described in Table 2.



Inspection Management

Manage your Inspections.

Inspection List

Show 10 entries

Bridge no.	Bridge name	Type	Assigned to	Assigned by	Assigned on	Deadline	Status	Action
54-014/00-013.22	Fifth Street Bridge	Initial	Rebecca Johnson	Irene Song	2022-03-01	2022-03-31	Awaiting Confirmation	Contact Inspector
07-005/00-016.61	Henrietta Bridge	Initial	Rebecca Johnson	Irene Song	2022-02-20	2022-12-22	Declined	View Comments
08-002/00-003.36	West Porter Creek Bridge	Initial	Rebecca Johnson	Irene Song	2022-02-20	2022-10-27	In Progress	Contact Inspector
44-003/00-002.58	Bay Bridge	Special	Rebecca Johnson	Irene Song	2022-02-20	2022-07-09	Awaiting Confirmation	Contact Inspector
52-007/00-000.07	Richard Snyder Memorial Bridge	Damage	Liam Davis	Noah Wilson	2022-01-07	2022-08-31	Awaiting Approval	Review
21-013/00-004.39	Berlin Bridge	Special	Liam Davis	Irene Song	2022-01-03	2022-01-28	Declined	View Comments
12-005/00-000.13	Arthur Bridge	Damage	Rebecca Johnson	Irene Song	2022-01-03	2022-06-30	Rejected	Reassign
51-005/01-001.98	Gaurdian Bridge	In-Depth	Rebecca Johnson	Noah Wilson	2022-01-03	2022-07-29	Awaiting Approval	Review
01-012/03-000.02	Laurel CK DK GRD 1	Initial	Rebecca Johnson	John Marshall	2021-12-01	2021-12-31	In Progress	Contact Inspector
04-013/02-003.21	Hecks Bridge	Initial	Rebecca Johnson	John Marshall	2021-12-01	2021-12-31	In Progress	Contact Inspector

Showing 1 to 10 of 15 entries

Previous 1 2 Next

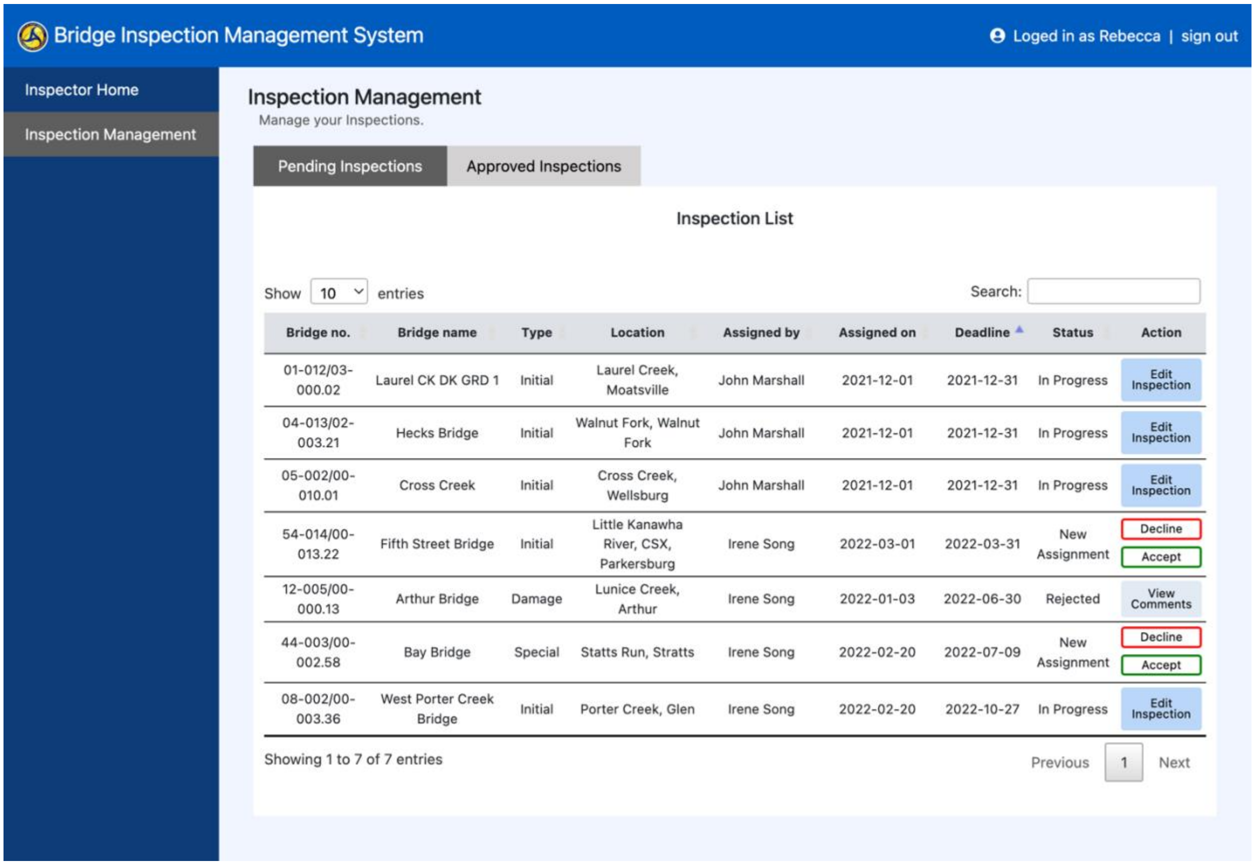
Figure 7. Inspection Management on the administrator's side

Inspection Status	*Description*
Awaiting Approval	The inspection report submitted by the inspector is awaiting final approval by the administrator.
Awaiting Confirmation	The assigned inspection is awaiting schedule confirmation from the inspector.
Declined	The inspector declined the assigned inspection.
In Progress	Inspection is in progress by the inspector.
Rejected	The inspection report submitted by the inspector was rejected by the administrator.

Table 2: Inspection status types

Besides, administrators can review inspection reports, and approved inspections are archived.

Inspectors can view the list of inspections assigned by the administrator and those approved. They can accept/reject the assigned inspections using the web application, which enables communication with the administrator regarding inspections. After completing the on-site inspection and data collection, the inspector can start generating an inspection report using the web interface, as shown in Figure 8.



Inspection Management

Manage your Inspections.

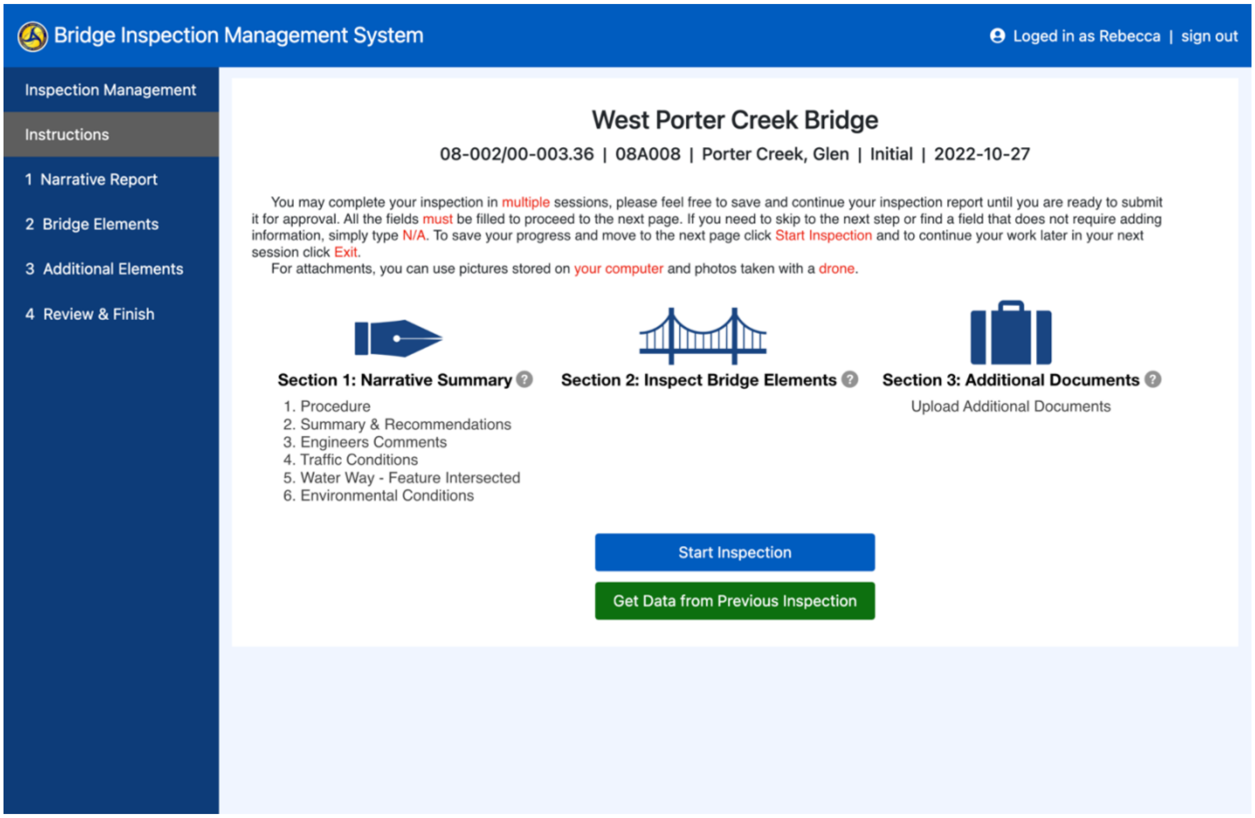
Inspection List

Bridge no.	Bridge name	Type	Location	Assigned by	Assigned on	Deadline	Status	Action
01-012/03-000.02	Laurel CK DK GRD 1	Initial	Laurel Creek, Moatsville	John Marshall	2021-12-01	2021-12-31	In Progress	Edit Inspection
04-013/02-003.21	Hecks Bridge	Initial	Walnut Fork, Walnut Fork	John Marshall	2021-12-01	2021-12-31	In Progress	Edit Inspection
05-002/00-010.01	Cross Creek	Initial	Cross Creek, Wellsburg	John Marshall	2021-12-01	2021-12-31	In Progress	Edit Inspection
54-014/00-013.22	Fifth Street Bridge	Initial	Little Kanawha River, CSX, Parkersburg	Irene Song	2022-03-01	2022-03-31	New Assignment	Decline Accept
12-005/00-000.13	Arthur Bridge	Damage	Lunice Creek, Arthur	Irene Song	2022-01-03	2022-06-30	Rejected	View Comments
44-003/00-002.58	Bay Bridge	Special	Statts Run, Stratts	Irene Song	2022-02-20	2022-07-09	New Assignment	Decline Accept
08-002/00-003.36	West Porter Creek Bridge	Initial	Porter Creek, Glen	Irene Song	2022-02-20	2022-10-27	In Progress	Edit Inspection

Showing 1 to 7 of 7 entries

Figure 8. Inspection Management on the inspector's side

The report generating interface implemented based on the actual WV bridge inspection report analysis consists of three sections: Narrative Summary, Inspection Findings of Bridge Elements, and Additional Documents. Figure 9 shows the instructions for creating the report. As the first step in generating a report, the inspector writes narrative summaries. The person in charge describes the inspection procedure, inspection summary, comments, traffic conditions, etc., and can attach pictures for each individual narrative item.



West Porter Creek Bridge

08-002/00-003.36 | 08A008 | Porter Creek, Glen | Initial | 2022-10-27

You may complete your inspection in multiple sessions, please feel free to save and continue your inspection report until you are ready to submit it for approval. All the fields must be filled to proceed to the next page. If you need to skip to the next step or find a field that does not require adding information, simply type N/A. To save your progress and move to the next page click Start Inspection and to continue your work later in your next session click Exit.

For attachments, you can use pictures stored on your computer and photos taken with a drone.

Section 1: Narrative Summary

1. Procedure
2. Summary & Recommendations
3. Engineers Comments
4. Traffic Conditions
5. Water Way - Feature Intersected
6. Environmental Conditions

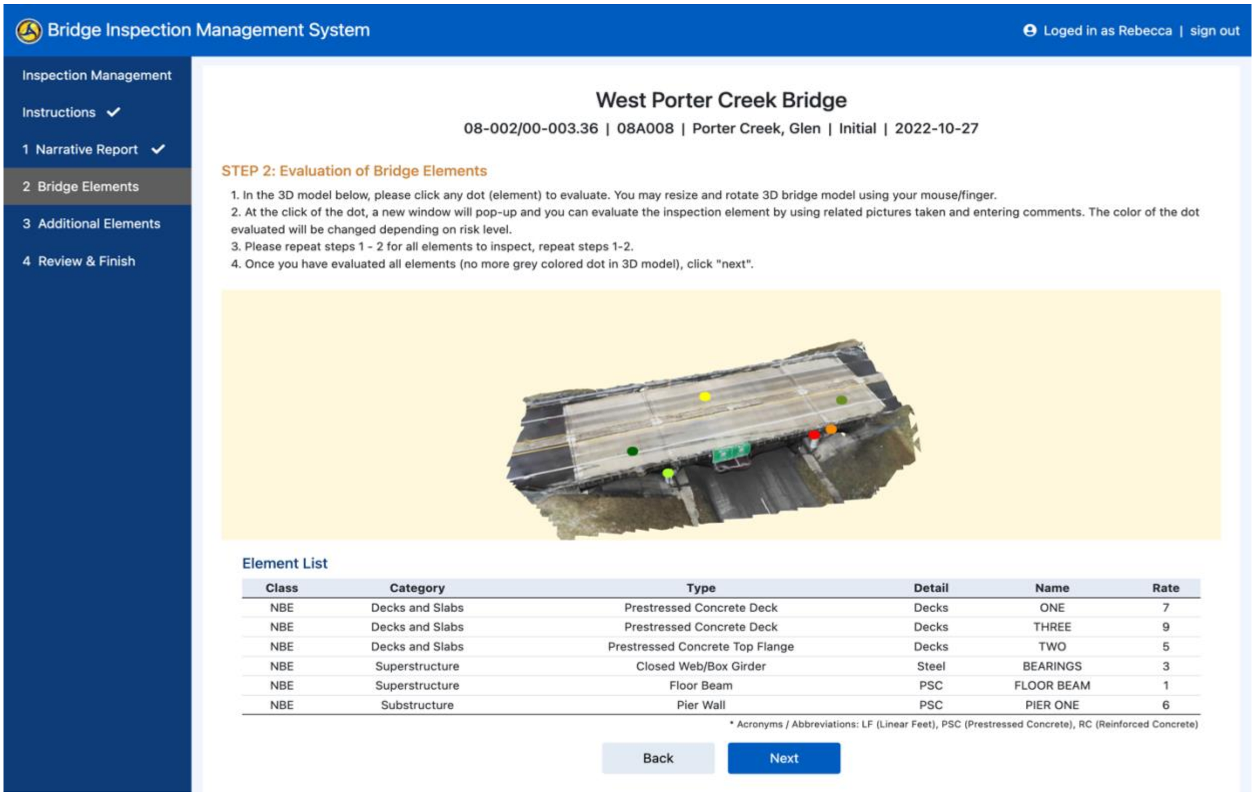
Section 2: Inspect Bridge Elements

Section 3: Additional Documents

Upload Additional Documents

Figure 9. Instructions for generating a bridge inspection report

Second, describing the inspection findings of bridge elements is a major part of generating a report. The inspector can use the memory device or database server in which the information collected in the field investigation stage is stored through the data collection module. As shown in Figure 10, each picture can be mapped to bridge elements in the 3D model based on GPS information. When each dot representing bridge elements is clicked, the basic information of the component, as well as photos with its note written by inspectors. Pictures having the same GPS information as the coordinate of each element are automatically selected. Since every bridge component also shows all sub-data of the image sets selected by the user, it can be added or excluded by the need of the official.



West Porter Creek Bridge

08-002/00-003.36 | 08A008 | Porter Creek, Glen | Initial | 2022-10-27

STEP 2: Evaluation of Bridge Elements

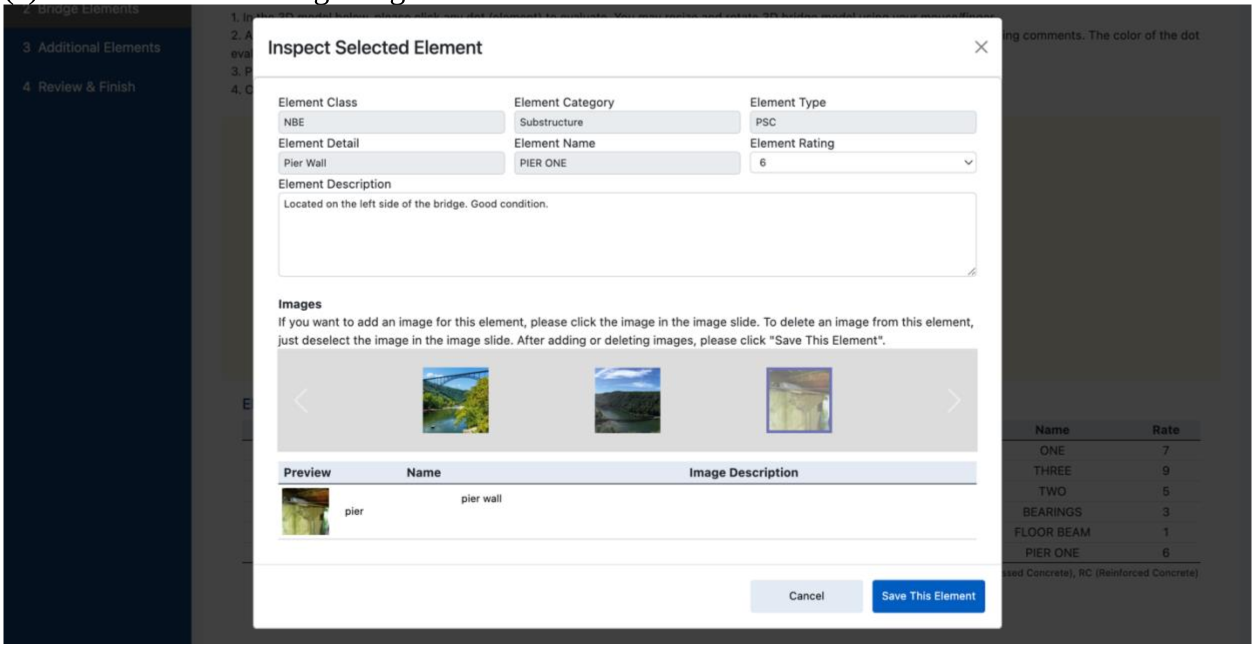
1. In the 3D model below, please click any dot (element) to evaluate. You may resize and rotate 3D bridge model using your mouse/finger.
2. At the click of the dot, a new window will pop-up and you can evaluate the inspection element by using related pictures taken and entering comments. The color of the dot evaluated will be changed depending on risk level.
3. Please repeat steps 1 - 2 for all elements to inspect, repeat steps 1-2.
4. Once you have evaluated all elements (no more grey colored dot in 3D model), click "next".

Element List

Class	Category	Type	Detail	Name	Rate
NBE	Decks and Slabs	Prestressed Concrete Deck	Decks	ONE	7
NBE	Decks and Slabs	Prestressed Concrete Deck	Decks	THREE	9
NBE	Decks and Slabs	Prestressed Concrete Top Flange	Decks	TWO	5
NBE	Superstructure	Closed Web/Box Girder	Steel	BEARINGS	3
NBE	Superstructure	Floor Beam	PSC	FLOOR BEAM	1
NBE	Substructure	Pier Wall	PSC	PIER ONE	6

* Acronyms / Abbreviations: LF (Linear Feet), PSC (Prestressed Concrete), RC (Reinforced Concrete)

(a) An overview of rating bridge elements



Inspect Selected Element

Element Class: NBE

Element Category: Substructure

Element Type: PSC

Element Detail: Pier Wall

Element Name: PIER ONE

Element Rating: 6

Element Description: Located on the left side of the bridge. Good condition.

Images

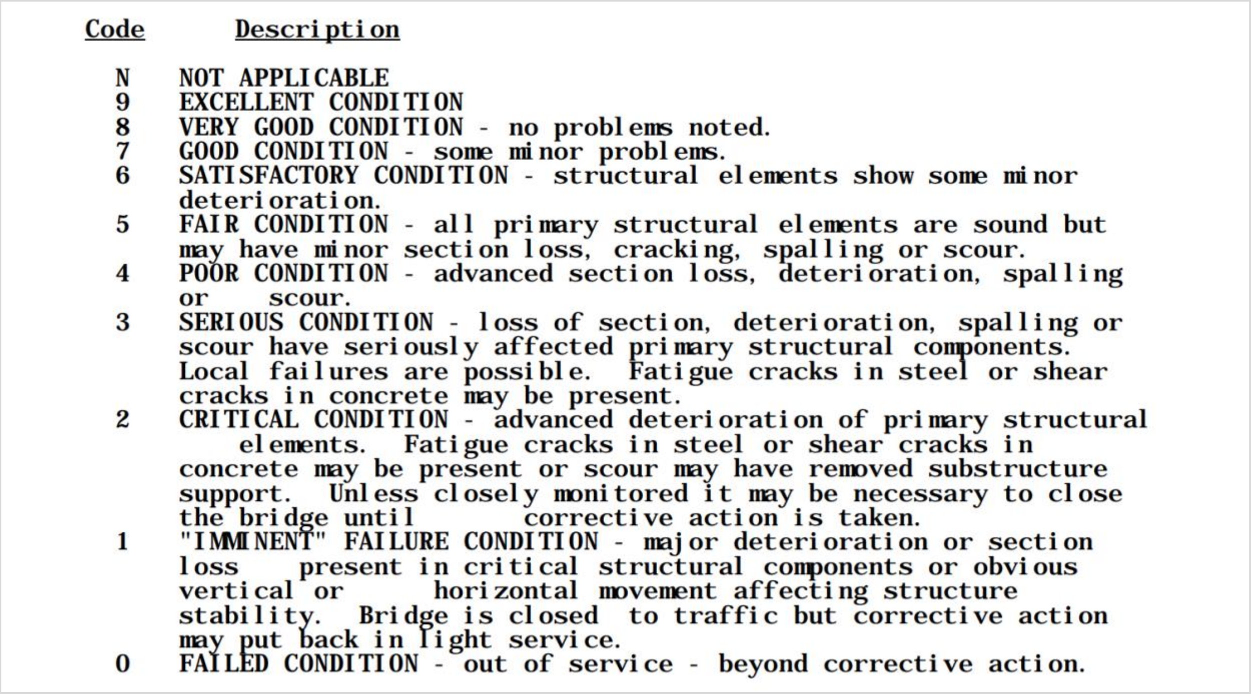
If you want to add an image for this element, please click the image in the image slide. To delete an image from this element, just deselect the image in the image slide. After adding or deleting images, please click "Save This Element".

Preview	Name	Image Description
	pier	pier wall

(b) Details of rating bridge elements

Figure 10. Inspection findings of bridge elements

This approach allows inspectors to choose the most suitable photos for inspection and edit notes related to the element. Inspectors can rate the safety level on a scale of 1 to 9 based on criteria established by the Federal Highway Administration (FHWA), and the classification of conditions is shown in Figure 11 (U.S. Department of Transportation Federal Highway Administration, 1995). Bridge elements marked with gray dots in the initial 3D model are displayed in different colors (1 – 3: red, 4 – 6: yellow, 7 – 9: green) depending on their rating. This feature enables intuitive analysis by visually displaying the condition of the bridge.



```
Code      Description

  N    NOT APPLICABLE
  9    EXCELLENT CONDITION
  8    VERY GOOD CONDITION - no problems noted.
  7    GOOD CONDITION - some minor problems.
  6    SATISFACTORY CONDITION - structural elements show some minor
       deterioration.
  5    FAIR CONDITION - all primary structural elements are sound but
       may have minor section loss, cracking, spalling or scour.
  4    POOR CONDITION - advanced section loss, deterioration, spalling
       or    scour.
  3    SERIOUS CONDITION - loss of section, deterioration, spalling or
       scour have seriously affected primary structural components.
       Local failures are possible.  Fatigue cracks in steel or shear
       cracks in concrete may be present.
  2    CRITICAL CONDITION - advanced deterioration of primary structural
           elements.  Fatigue cracks in steel or shear cracks in
       concrete may be present or scour may have removed substructure
       support.  Unless closely monitored it may be necessary to close
       the bridge until       corrective action is taken.
  1    "IMMINENT" FAILURE CONDITION - major deterioration or section
       loss    present in critical structural components or obvious
       vertical or      horizontal movement affecting structure
       stability.  Bridge is closed  to traffic but corrective action
       may put back in light service.
  0    FAILED CONDITION - out of service - beyond corrective action.
```

Figure 11. Condition Ratings (U.S. Department of Transportation Federal Highway Administration, 1995)

As the last step of generating an inspection report, the inspector can use the file upload function to add documents and then review the final contents of the report. The review page in the web interface also provides the PDF version that will be generated, similar to the bridge inspection report used by the state DoT. This preview function allows inspectors to obtain soft and hard copies of the final report.

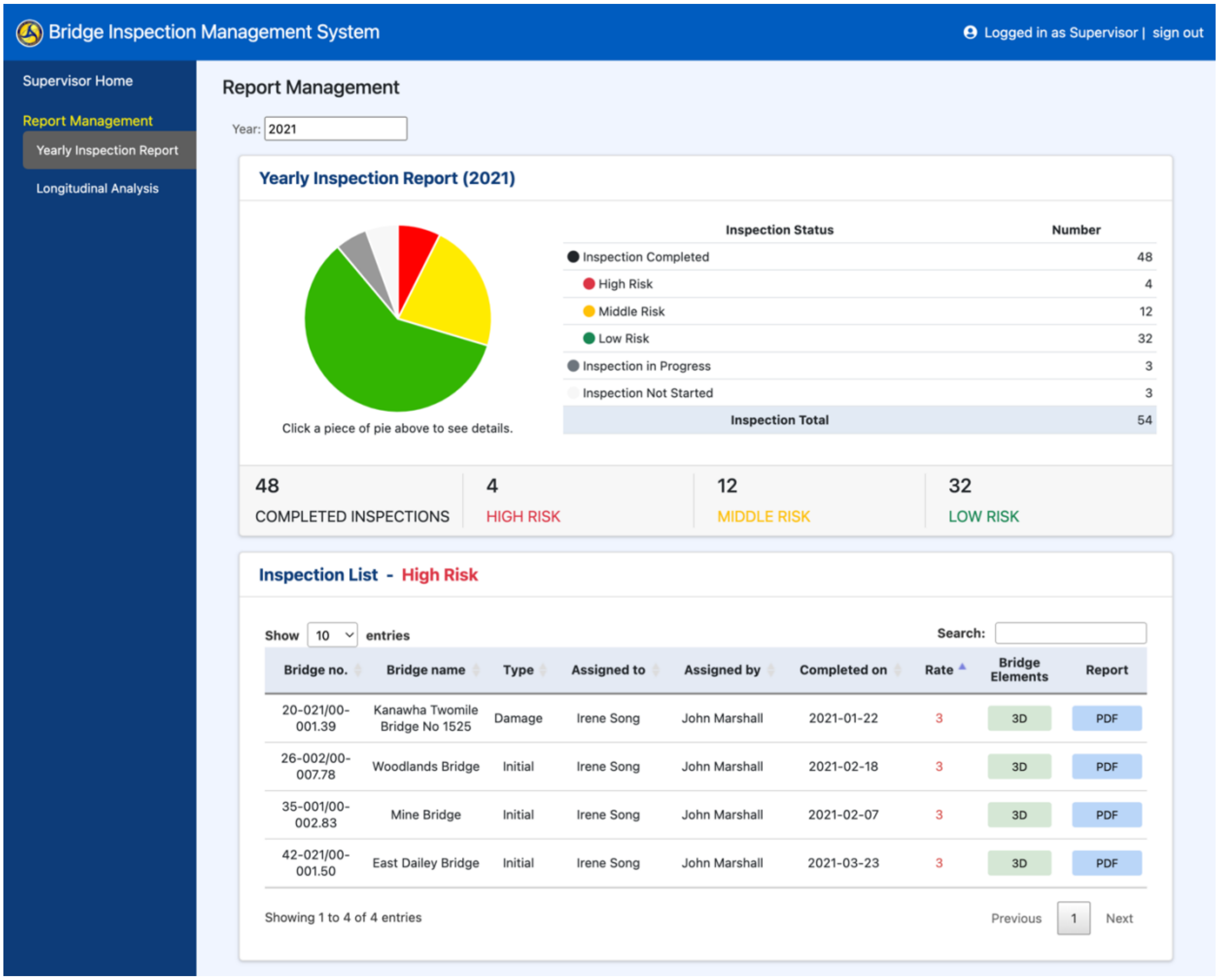
Inspector management

Inspector Management provides a user interface for personnel management, such as adding inspectors or revoking their privileges to the system. Administrators can create new inspector accounts. Inspector information can be updated or deleted. This process allows new inspectors to gain access to the system.

Report Management

Report Management contains visualization features and statistical functions for data analysis. The supervisor can use the Yearly Inspection Report Tool to view the overall status of the bridge inspections, including the number of inspections performed per year and the categorized bridge list by the risk rate. The assessed risk level by year for the selected bridge can be tracked and checked through the Longitudinal Analysis Tool.

The Yearly Inspection Report displays the number of inspections assigned and performed in a particular year. Figure 12 shows the bridge inspection statistics by year displayed as a pie chart. Supervisors can visually check how many bridges are classified by risk rate and clicking on each risk label in the pie chart lists the bridges in that category. This list provides drill-down functions. The web application provides a 3D model containing bridge elements marked dots of different colors according to the condition rating and includes a report of the inspection in PDF format. Supervisors can save it in digital format document or print this document.



Bridge Inspection Management System

Logged in as Supervisor | sign out

Supervisor Home

Report Management

Yearly Inspection Report

Longitudinal Analysis

Report Management

Year: 2021

Yearly Inspection Report (2021)

Inspection Status	Number
● Inspection Completed	48
● High Risk	4
● Middle Risk	12
● Low Risk	32
● Inspection in Progress	3
○ Inspection Not Started	3
Inspection Total	54

Click a piece of pie above to see details.

48	4	12	32
COMPLETED INSPECTIONS	HIGH RISK	MIDDLE RISK	LOW RISK

Inspection List - High Risk

Show 10 entries

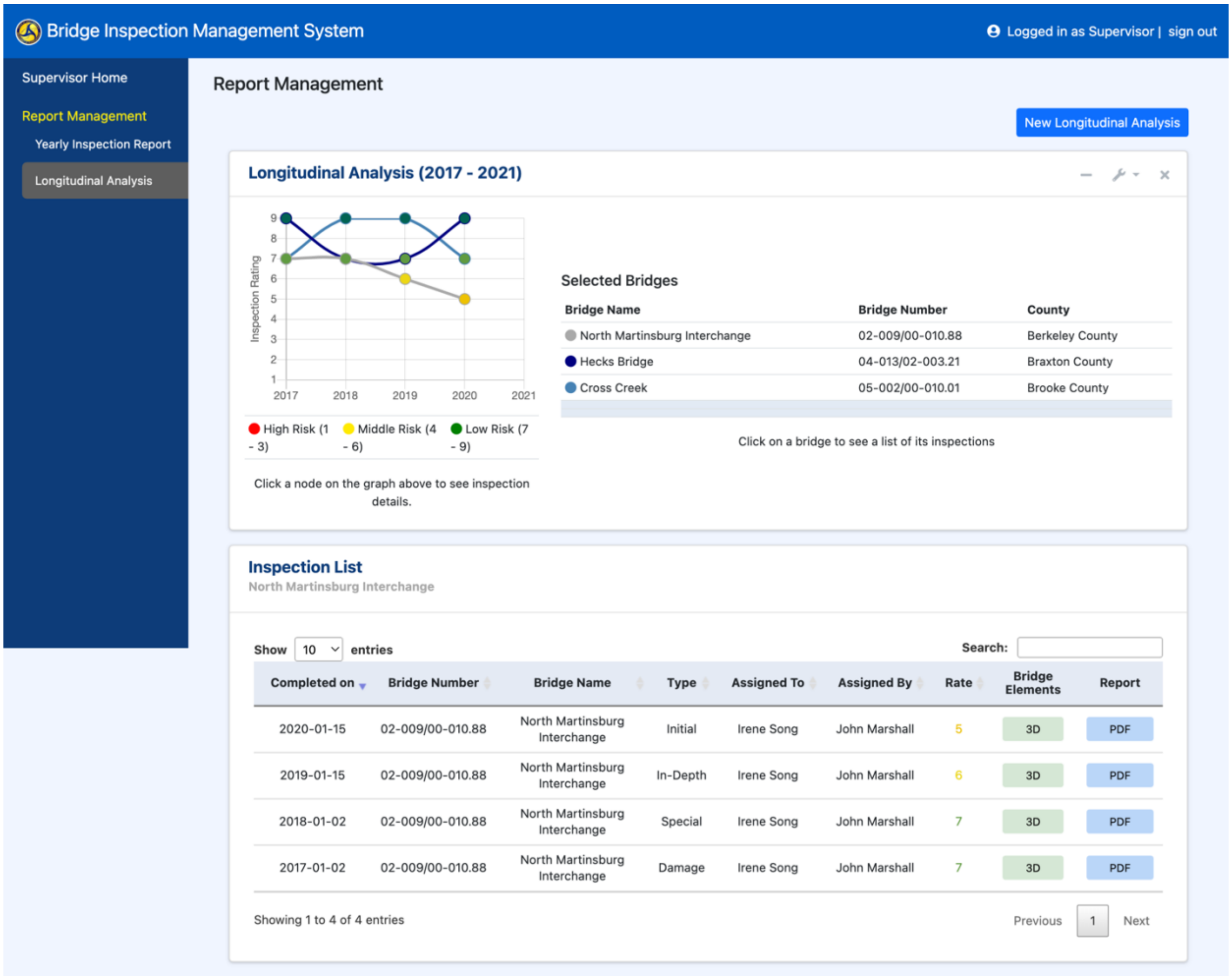
Search:

Bridge no.	Bridge name	Type	Assigned to	Assigned by	Completed on	Rate	Bridge Elements	Report
20-021/00-001.39	Kanawha Twomile Bridge No 1525	Damage	Irene Song	John Marshall	2021-01-22	3	3D	PDF
26-002/00-007.78	Woodlands Bridge	Initial	Irene Song	John Marshall	2021-02-18	3	3D	PDF
35-001/00-002.83	Mine Bridge	Initial	Irene Song	John Marshall	2021-02-07	3	3D	PDF
42-021/00-001.50	East Dailey Bridge	Initial	Irene Song	John Marshall	2021-03-23	3	3D	PDF

Showing 1 to 4 of 4 entries

Previous 1 Next

Figure 12. Report Management on the supervisor's side – Yearly Inspection Report


Bridge Inspection Management System
Logged in as Supervisor | sign out
Supervisor Home
Report Management
Yearly Inspection Report
Longitudinal Analysis
Report Management
New Longitudinal Analysis
Longitudinal Analysis (2017 - 2021)
Inspection Rating
9
8
7
6
5
4
3
2
1
2017
2018
2019
2020
2021
High Risk (1 - 3)
Middle Risk (4 - 6)
Low Risk (7 - 9)
Click a node on the graph above to see inspection details.
Selected Bridges
Click on a bridge to see a list of its inspections
Inspection List
North Martinsburg Interchange
Show 10 entries
Search:
Showing 1 to 4 of 4 entries
Previous
1
Next

Bridge Name	Bridge Number	County
● North Martinsburg Interchange	02-009/00-010.88	Berkeley County
● Hecks Bridge	04-013/02-003.21	Braxton County
● Cross Creek	05-002/00-010.01	Brooke County

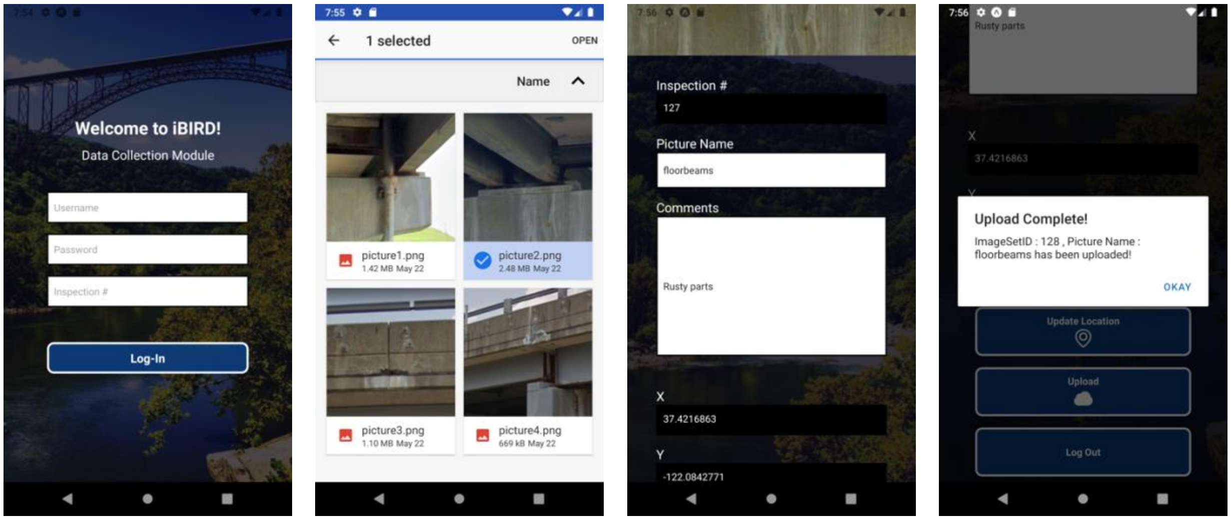
Completed on	Bridge Number	Bridge Name	Type	Assigned To	Assigned By	Rate	Bridge Elements	Report
2020-01-15	02-009/00-010.88	North Martinsburg Interchange	Initial	Irene Song	John Marshall	5	3D	PDF
2019-01-15	02-009/00-010.88	North Martinsburg Interchange	In-Depth	Irene Song	John Marshall	6	3D	PDF
2018-01-02	02-009/00-010.88	North Martinsburg Interchange	Special	Irene Song	John Marshall	7	3D	PDF
2017-01-02	02-009/00-010.88	North Martinsburg Interchange	Damage	Irene Song	John Marshall	7	3D	PDF

Figure 13. Report Management on the supervisor's side – Longitudinal Analysis

Figure 13 shows the Longitudinal Analysis function. This feature contains a graph of the risk trend of the bridge within the selected time frame. When a specific bridge is selected in this graph, the system returns a list of inspections by year. This list contains 3D models with color-coded risk of bridge elements and an inspection report for each year.

4.2 Mobile Application

To provide a smooth on-site inspection process, a mobile application compatible with the portable device controlling the drone has been developed. The use of React Native, which can also be used cross-platform, was considered. For this purpose, the Expo framework was used, and it allows JavaScript codebase. The user interface was implemented in JavaScript. Calls to the PHP API were utilized to communicate with the web application's server and database. This mobile application can use the POST method to send images and information through the API to the server filesystem and database.



Inspection # 127

Picture Name floorbeams

Comments Rusty parts

X 37.4216863

Y -122.0842771

Upload Complete!

ImageSetID : 128 , Picture Name : floorbeams has been uploaded!

(a) Login (b) Select a picture (c) Write an inspection note (d) Upload the data

Figure 14. Collecting Inspection Data using Mobile Application

Figure 14 describes the process of collecting inspection data using the mobile application according to the task sequence. Inspectors access the system by entering their credentials and assigned inspection ID. By introducing the traditional login function with sessions, user authentication has been strengthened and the security of the system has been improved. An authorized user takes a picture of a bridge using a UAV and then selects a picture stored in the IoT device memory or takes a picture using the mobile interface. The inspector can load a photo into the application and add its name with an associated description. Along with user-entered information, pictures, including GPS and metadata such as date and time, can be stored in the memory of the IoT device or uploaded to a remote data server. The stored data transmitted to the remote server can be accessed by web applications, which can be used to generate inspection reports.

4.3 Simulation of PUF-based Mutual Authentication Algorithm

A mutual authentication scheme has been implemented to ensure secure data communication between the server and IoT devices. This thesis adopts the PUF-based algorithm proposed by Aman et al. (2017). In this research, the server-side language is PHP, and the IoT device uses JavaScript. Authentication messages are created and communicated using encryption methods and computations compatible with each language. For encryption, the OpenSSL library was used on the server-side, and the crypto-js library was used on the IoT side.

To simulate the PUF-based algorithm, several assumptions were made as follows.

1) A custom function is used to generate a response using a challenge and PUF.

2) A random 32-bit binary value was assigned as the PUF value.

3) Table 3 shows the notations for describing the algorithm.

Notation	***Description***
ID_A	Identifier of the IoT device
ID_S	Identifier of the Server
N_0	32-bit initial nonce
C^i, C^{i+1}	Challenge at the i-th, $(i+1)$th iteration
R^i, R^{i+1}	Response of the Challenge C^i, C^{i+1}
RN, N_A	32-bit random nonce
$\|$	Concatenation operator
$\{\ \}_{R^i}$	Encryption using key R^i
M_A, M_S	128-bit encrypted message for ID_A, ID_S
MAC_A, MAC_S	Message authentication code for ID_A, ID_S
$\oplus$	Bitwise Exclusive OR (XOR) operator
F_{PUF}	A custom function using PUF
$h(\ )$	Hash function

Table 3: Notations for PUF-based mutual authentication algorithm

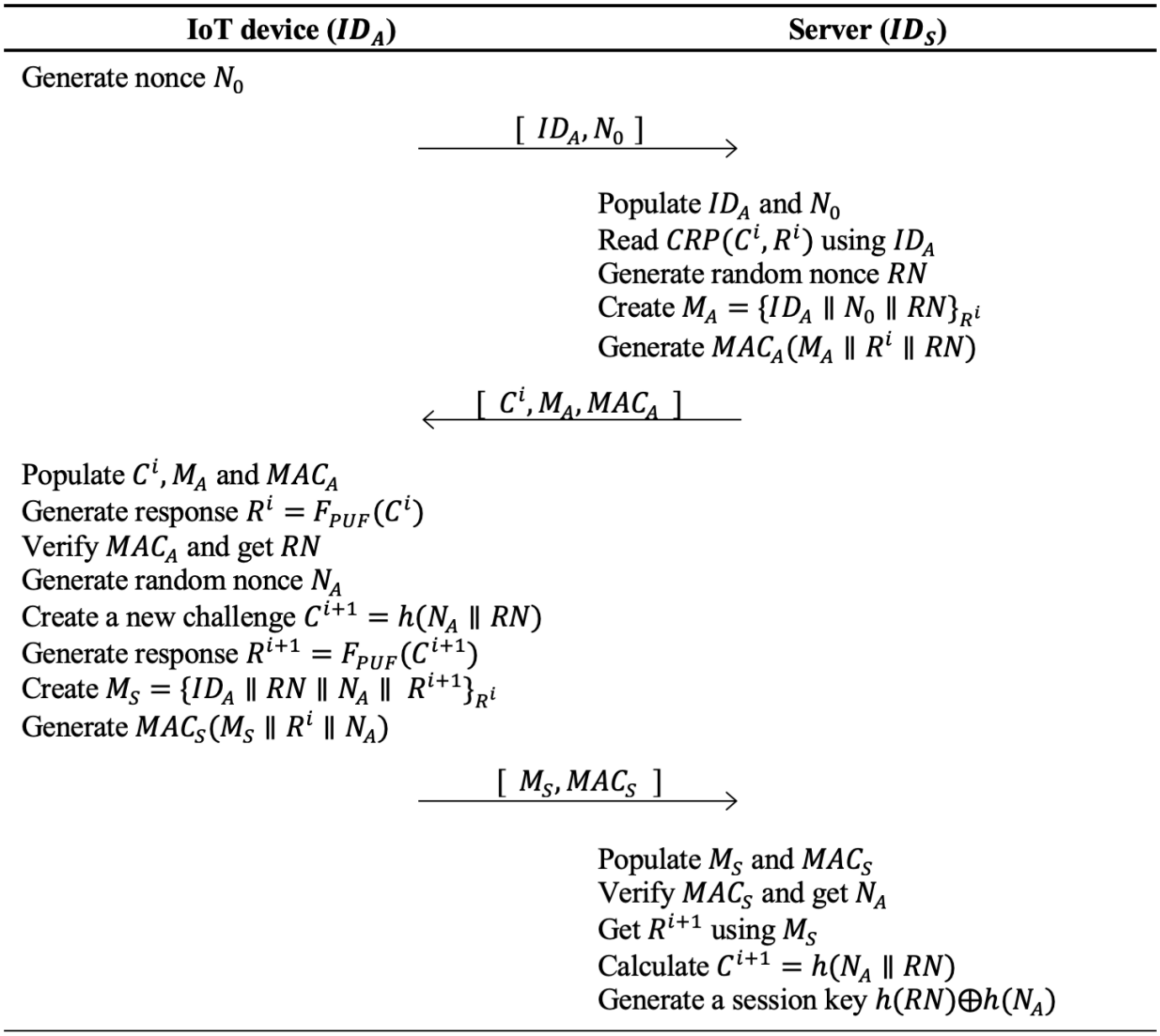
The PUF-based light-weight mutual authentication algorithm simulated in this thesis is summarized in Figure 15. This protocol consists of four steps.

1) The IoT device (ID_A) generates a nonce N0 in the traditional login process which uses a password method and then sends this value to the server (ID_S) with the ID_A.
2) The server reads the CRP (C^i, R^i) that they already know corresponding to the ID_A. For the upcoming message generation step, a 32-bit random nonce RN is generated, and ID_A, N_0, and RN are concatenated. This concatenated value is encrypted using the response R^i hashed using Secure Hash Algorithm (SHA)-256 as a key to generating an encrypted message M_A. For this, Advanced Encryption Standard (AES)-256 in Cipher Block Chaining (CBC) mode is used. Then, the message M_A, the response R^i, and the nonce RN are concatenated to generate MAC_A, the code that authenticates the message. The server sends the challenge C^i, the message M_A, and the authentication code MAC_A to the IoT device.
3) The IoT device generates a response R^i using the challenge C^i received from the server and the unique fingerprint PUF. This paper applies a bitwise XOR of the PUF to a challenge as a custom function for generating a response. For MAC verification, the response R^i is converted into a hash value using SHA-256. The device concatenates the message M_A and its hashed response R^i, removing the part equal to this value in the MAC_A. At this time, if MAC_A has the same value as before the removal step, MAC verification fails. This means that the response R^i of the server and the response R^i calculated by the IoT are different, so they have different PUF values. Since the remaining part is a random nonce RN generated by the server, the IoT device obtains the nonce RN value after the successful removal process. Next, a 32-bit

random nonce N_A is generated, and this nonce N_A and random nonce RN are concatenated for the following step. This linked value creates a new challenge C^{i+1} by SHA-256 hash. Using C^{i+1} and the PUF, a new response R^{i+1} is calculated. Then, ID_A, RN, N_A, and R^{i+1} are concatenated, and this value is encrypted using the SHA-256 hashed response R^i as a key to generate an encrypted message M_S. For this, AES-128 in CBC mode is used. The message M_S, the response R^i, and the nonce N_A are concatenated to generate MAC_S, a code that authenticates the message. Finally, the IoT device sends the encrypted message M_S and the authentication code MAC_S to the server.

4) The server concatenates the message M_S and the hashed response R^i, removing the part equal to this value in MAC_S. At this time, if MAC_S has the same value as before the removal step, MAC verification fails. This means that the response R^i of the server and the response R^i calculated by the IoT are different. They, therefore, have different PUF values. Since the remaining part is a random nonce N_A generated by the IoT device, the server obtains a nonce N_A value after the successful removal process. Next, the message M_S is decrypted by using AES-128 in CBC mode with the SHA-256 hashed response value R^i as the key. If decryption is not performed successfully, it means that the client has a different value for R^i. Thus, authentication fails. The server concatenates ID_A, RN, and N_A to remove the same part as this value from the decoded M_S. If this removal is successful, the server gets a new response R^{i+1} calculated by the IoT device. The random nonce N_A and the random nonce RN are concatenated for the next step, and this linked value generates a new challenge C^{i+1} by hashing using SHA-256. If all steps are successful, the server applies XOR to the random nonce RN and

the random nonce N_A respectively hashed with SHA-256 and then stores them in the session.



IoT device (ID_A) | **Server (ID_S)**

Generate nonce N_0

$\xrightarrow{[\ ID_A, N_0\ ]}$

Populate ID_A and N_0
Read $CRP(C^i, R^i)$ using ID_A
Generate random nonce RN
Create $M_A = \{ID_A \parallel N_0 \parallel RN\}_{R^i}$
Generate $MAC_A(M_A \parallel R^i \parallel RN)$

$\xleftarrow{[\ C^i, M_A, MAC_A\ ]}$

Populate C^i, M_A and MAC_A
Generate response $R^i = F_{PUF}(C^i)$
Verify MAC_A and get RN
Generate random nonce N_A
Create a new challenge $C^{i+1} = h(N_A \parallel RN)$
Generate response $R^{i+1} = F_{PUF}(C^{i+1})$
Create $M_S = \{ID_A \parallel RN \parallel N_A \parallel\ R^{i+1}\}_{R^i}$
Generate $MAC_S(M_S \parallel R^i \parallel N_A)$

$\xrightarrow{[\ M_S, MAC_S\ ]}$

Populate M_S and MAC_S
Verify MAC_S and get N_A
Get R^{i+1} using M_S
Calculate $C^{i+1} = h(N_A \parallel RN)$
Generate a session key $h(RN) \oplus h(N_A)$

Figure 15. Summary of the Simulated PUF-based Mutual Authentication Algorithm

This lightweight algorithm for mutual authentication ensures data integrity by using encrypted messages and hashed values. It also enables device authentication. The server can decide whether to trust the device based on whether it is authenticated or not. This scheme, therefore, provides reliability for the data transmitted by the authenticated device. Since the database only stores data transmitted by legitimate IoT devices, security issues caused by improper data insertion can be resolved. Furthermore, Aman et al. (2017), who proposed the lightweight algorithm simulated in this system, provided a security analysis of this protocol using Mao and Boyd logic (Mao & Boyd, 1993). This proved that the applied mutual authentication algorithm is safe against all major security attacks, including spoofing, man-in-the-middle, eavesdropping, etc (Aman et al., 2017).

4.4 Database

The database is designed to be accessible by web and mobile applications. Through the requirements analysis, relations between entities and properties have been defined. MySQL Workbench was used to design the relational database, resulting in an Entity Relationship Diagram (ERD). Figure 16 shows the designed database, and more detailed information can be found in *Appendix C*. The stored procedure approach is adopted for query security. The generated physical schema has migrated to the server.

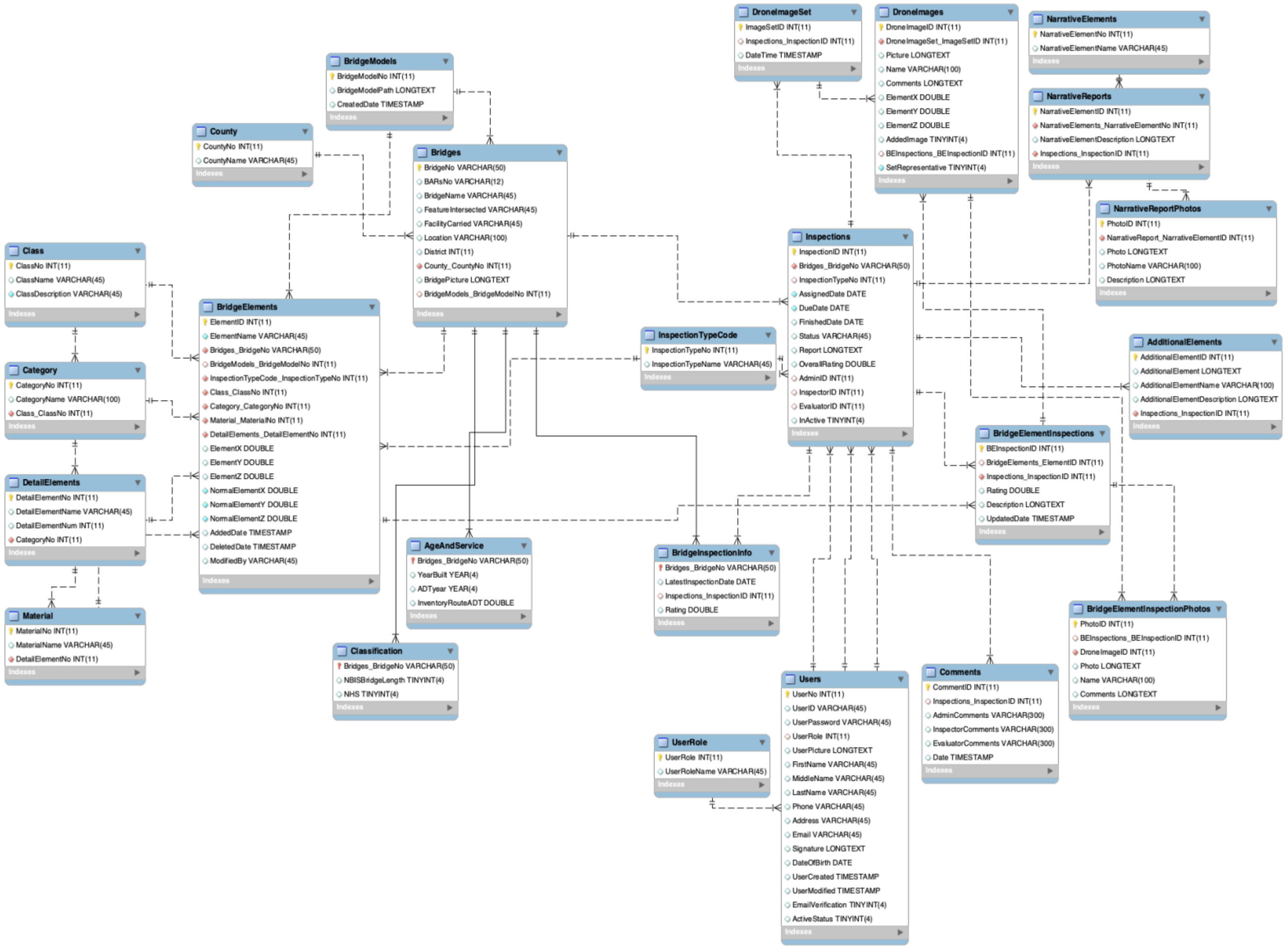


Figure 16. Entity relationship diagram of the implemented database

The database consists of twenty-four tables. Among these, notable tables are Inspections, Bridges, and Bridge Elements. The ‘inspections’ table contains several basic information about the inspection, and the primary key is *inspectionID,* which is automatically incremented. *BridgeNo, InspectionTypeNo, AdminID, InspectorID,* and *EvaluatorID* are foreign keys, forming a relationship with other tables. *BridgeNo* cannot be null. The ‘bridges’ table contains basic information about bridges, and the primary key is *BridgeNo*. *CountyNo* and *BridgeModelNo* are foreign keys, and *BARsNo*, a unique bridge management number, cannot have duplicate values. The ‘bridge elements’ table contains overall data about bridge elements, and the primary key is *ElementID*. *BridgeNo* and *InspectionTypeNo* make each row unique and are foreign keys. *ClassNo, CategoryNo, MaterialNo, DetailElementNo*, which are element’s information, are also foreign keys and are linked to each table. These foreign key values cannot be null. The current database schema was designed based on an analysis of the National Bridge Inspection Standards (NBIS). It is, thus, capable of defining inspection for various types of bridges that are currently in use in the United States.

This database is designed to reduce redundancy data between tables through normalization. In the first normalization process, each column is defined to have only one value. For example, one inspector can create multiple inspections. If data is organized depending on users, one row should own multiple columns. To prevent this, the inspection table applied a method to have different rows based on a unique inspection ID rather than for each inspection user, and this made every column have only one column value. In the same vein, a bridge has multiple bridge elements. If the bridge element table is grouped by bridge ID, multiple values can belong to one column. With this in mind, the devised database is placed in different rows in the bridge element table, even if the same bridge identification number.

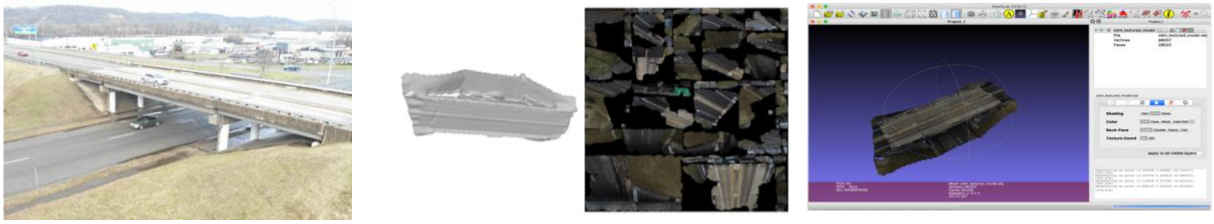
The proposed database does not use more than one primary key for each table. This satisfies a fully functional dependency on all columns. Finally, transition dependency was eliminated. An inspection, for instance, requires not only a user's unique ID to identify who is in charge but also details such as the roles of the users. Instead of listing each user's details in the inspector table, by separating the user table from the user role table, the Third Normal Form (3NF) is satisfied. As a result, the data redundancy was reduced through the third normalization process.

A variety of data is used in the bridge inspection report. The actual bridge inspection report was analyzed, and the information was divided into structured data and unstructured data. For structured data, a generally accepted length was applied in consideration of the format. An example of unstructured data is the description that each item in the narrative report contains. Because the length of them was not regulated by the transportation department. For these unstructured data, the proposed database uses the LONGTEXT type to accept input up to 2^{32} characters (ORACLE, 2022).

4.5 3D Modeling of Bridge

In the previous study in this thesis, iBIRD (Song et al., 2022), field tests were performed in compliance with federal and state regulations and laws to generate an initial 3D model of the bridge. The target bridge was photographed by flying a UAV. The shooting was repeated several times to improve data quality. The visual data obtained in this method were extracted as images through frame division, and pictures were selected so as not to exceed the maximum processing number of 120. Each image contained more than 85% connected shapes and it is an important factor in improving the accuracy of the 3D model. This selected series of pictures were converted to an object file via ODM in a docker environment. The object file and texture files generated as a result of this modeling process were integrated using MeshLab, and the 3D model of the bridge was improved by removing unnecessary areas.

This thesis added an advanced retouching through Blender and conversion to glb format while maintaining the overall framework of 3D modeling proposed by iBIRD (Song et al., 2022). Previous research used Three.js to provide a 3D model manipulation function, which made the program heavy and slow. To improve this issue, an API, <model-viewer>, was adopted in this research. This approach significantly reduced the number of lines of code and remarkably shortened the web loading time. These improvements have the advantage of making it possible to create more sophisticated bridge models but also providing easy maintenance. Furthermore, it was shown that even when using 3D models obtained from external sources, they can be applied to the system through a simple format conversion process. It proves the scalability of the proposed schema.



(a) Picture of actual bridge (b) Model created by ODM (c) Refined Model by MeshLab

Figure 17. The 3D modeling process of the bridge

CHAPTER 5: SECURITY AND THREAT ANALYSIS

It is necessary to clarify exactly what is meant by “trust.” Throughout this thesis, the term “trust” refers to the state in which users believe that the platform is safe for data communication by ensuring that information requiring a certain level of security, such as bridge inspection data, is not leaked or tampered with by unauthorized entities. In other words, a trusted platform means having an appropriate security medium to prevent information leakage and tampering by malicious subjects. It is an important part to set the level of cybersecurity for the implementation of a trusted platform. Various entities are involved in the bridge inspection system using UAVs and the threat factor is different for each entity. These threats may have different security levels or security baselines that can be applied to each subject.

The proposed schema has adopted the ZT architecture for threat analysis and security baseline setting. According to the definition of the National Security Agency (NSA, 2021), the ZT model is a security schema designed based on the assumption that threats exist without distinction between inside and outside the network. In other words, the model is based on the principle that threats can arise anywhere in a conventional network. This security model improves the security of data and systems by removing implicit trusts within the network and continuously verifying them. In the same vein, the Department of Defense (DOD) argues that a classic security strategy divided into multiple layers is ineffective against resource-rich intruders and proposes a ZT strategy to counter persistent cyber threats (Joint DISA/NSA Zero Trust Engineering Team, 2021). In line with these latest trends, this proposed schema assumes all entities as untrusted objects and analyzes the threats to each entity in terms of confidentiality, integrity, and availability (CIA) required in cybersecurity. The threats mentioned in this chapter can change according to the business environment, and the built-in security methods according to the analyzed threats can be replaced in the future depending on the change in the situation or to provide better stability.

5.1 User Security

Human resources accessing the system can be a major security threat. If unauthorized users access the system, there is a risk of tampering with the information or using it with malicious intentions. In other words, the confidentiality of data may not be maintained due to access by users with bad intentions. The proposed system handles bridge information and bridge inspection data. Basic bridge information, such as the bridge's name and location, is open to the public, but inspection data can be sensitive information as it describes the bridge's weaknesses. If confidentiality is not maintained, these vulnerabilities can be exploited by terrorists, which can lead to infrastructure collapse. In addition, access by users with malicious intentions can be a threat to integrity and availability. If the bridge data is changed without permission, it may provide incorrect inspection results for the bridge. This may affect the budget distribution and cause economic damage but also measures may not be taken in a timely manner for bridges in which actual danger is found due to incorrect inspection information. This can compromise integrity and availability.

In summary, due to the characteristic of bridge inspections that identify vulnerabilities in critical infrastructure, information leakage and manipulation can be serious problems. In view of this issue, the proposed platform subdivides the roles of users according to their tasks and controls access by granting the least privileges according to the roles. Depending on the authority, the scope of access to the system and the functions that can be used are limited, and this is strictly managed through authentication.

In this platform, authorized workers assumed that credentials were registered in the system in the pre-registration stage by the system administrator. The workers must be authorized officials in accordance with the transportation department’s internal policy. For example, supervisor privilege is given to the department’s chair, and administrator privileges allow access to the person who oversees inspections. Inspector authorities are limited to those who direct actual field work and generate reports. UAV pilots should be department officials with drone pilot certificates issued by the FAA.

For human entities to access the system, they are required to authenticate with a password. The password is encrypted and sent to the server and is stored as a SHA1 hash value, 40 hexadecimal digits long, in the database. The current hash function for passwords can be improved to make password guessing more difficult by adding a salt, an arbitrary string. The real accounts other than demonstration accounts use a password of at least 15 characters in length, and this password is considered a complex string containing both uppercase and lowercase letters and numbers. For better security in the future, user authentication can be strengthened by introducing Multi-Factor Authentication (MFA) authentication using email, text messages, and one-time passwords (OTP). Alternatively, it can be extended to a state authentication system, and a commercial authentication system provided by technology-leading companies can be introduced.

Verification of legitimate users also lowers the probability of system changes by unauthorized users. Consequently, the appropriate access control and least privilege principles applied to this scheme ensure confidentiality, integrity, and availability.

5.2 Hardware Security

Various hardware is involved in the bridge inspection scheme. This hardware includes client devices such as IoT devices and desktops and UAVs. The factors that make it difficult for hardware to ensure confidentiality, integrity, and availability are theft, use of unauthorized devices, or physical damage. For instance, the theft of an IoT device can result in the leakage of key inspection information, such as inspection notes temporarily stored on the machine. This can be a reason that makes it difficult to maintain confidentiality. In addition, if the bridge management system can be accessed through the use of unauthorized devices, unpredictable user behavior like data injection can pose a threat to the system. This can affect data integrity. Loss or breakage of UAVs and IoT devices can make it difficult to collect bridge inspection data and therefore not guarantee availability.

Considering these issues, countermeasures against physical threats and authentication for legitimate devices were considered when designing the proposed platform. First, it is assumed that the organization has established a set of policies for device management. All hardware in the proposed framework is assumed to be work devices. The devices that are monitored and managed by state officials are only used, and this means the use of secure hardware specified in accordance with the department’s internal security regulations. UAVs and IoT devices should be stored in a secure location to prevent theft, except when used in the field. The office where the desktop is installed may be a space that has closed-circuit televisions (CCTVs) and uses a security access key to limit user access. To prevent further security threats, it is assumed that only approved software can be installed on all hardware and that the devices are using the latest security patches. IoT and desktop devices should be set to lock the screen after a certain amount of time. Moreover, the hardware can be checked to ensure normal operation on a regular basis. In the future, full-disk encryption may also be considered. As a non-repudiation feature, access control can be added by logging device lists and access to devices.

Next, the proposed framework performs device authentication for IoT devices through the adoption of PUF-based algorithms. This algorithm implements mutual authentication of two entities by exchanging encrypted messages between an IoT device and a remote server and checking the suitability of the values. Messages and authentication code values used in this process are changed into ciphertext through hash function or encryption method and then communicated. This communication mechanism is also effective against man-in-the-middle attacks. It gives integrity to the system and provides authentication that verifies the entitlement of entities to access information, as well as includes non-repudiation capabilities.

Being prepared for physical threats and introducing user authentication mediums for legitimate devices ensures confidentiality and integrity and provides availability. The proposed system ensures authorization by giving permission to legitimate devices, verifies the conformity of the entities by introducing an authentication process, and has the accounting property by adopting access control over access history. The platform, thus, meets the authentication, authorization, and accounting security framework.

5.3 Software Security

In this thesis, the software includes intangible assets such as servers, implemented web and mobile applications, and databases. The factors that make it difficult for software to ensure confidentiality, integrity, and availability include the use of untrusted software and the lack of encryption policies for sensitive data. If untrusted software is used, input by inspectors or administrators can be intercepted, which can create confidentiality issues. If encryption for sensitive data is not in place, internal data can be leaked or easily changed by external objects. This affects confidentiality, integrity, and availability.

The web application of the proposed platform was hosted on a remote server. Considering this environment, it is assumed that access to the web application is accessed through a URL using the HTTPS method. In the future, the implementation of an internal server in the business unit can improve the reliability of the platform by making it accessible only from the intranet. In the case of the mobile application, a system manager directly installs the program on the device during the deployment stage to ensure safety. The system manager is an official who oversees the system in the department and is assumed to be a trusted person who has the original application installation files.

The database designed for this framework stores sensitive information such as passwords as hash values. This is a secure tool that minimizes damage by making it difficult to infer the plaintext even if the database is leaked. The use of hash functions provides confidentiality to the system. As an extension of the database, a stored procedure method is used in which Structured Query Language (SQL) is defined on the server. This hides the textual format query from the program code, making inference highly complex. It, therefore, prevents SQL injection attacks that can occur on the client-side or activities that manipulate SQL by analyzing code. That is, it not only ensures integrity by preventing the database from being changed by unauthorized users but also improves the security of the overall database. Besides, the proposed framework assumes regular backups of the database. This prevents data loss due to security breaches, allowing data to be provided in a timely manner for users. This ensures the availability of data. In addition, the mobile application proposed a method of storing the collected inspection data by transmitting it to a remote server in the field inspection stage. This prevents the loss of data availability due to the loss or theft of the inspector’s physical tools, which has been an issue in the traditional bridge inspection.

Providing legitimate software and including encryption functions and backup policies in the database maintains confidentiality, ensures integrity, and provides availability. In this chapter, the threat and security analysis of the proposed schema were presented in terms of user, hardware, and software. To build a trusted platform, the threats to each entity constituting the system were analyzed, and then the proposed system’s security baseline and security methods were presented to counter the potential threats.

CHAPTER 6: DISCUSSION

The fundamental goal of this research was to identify the issues of traditional bridge inspection and to devise a cost-effective and trusty bridge inspection schema that can replace the current method. To this end, visual inspection reports and bridge inspection manuals from federal, state, and local transportation agencies were analyzed. Based on this, Trusted-BIMS, a trusted bridge inspection framework using UAV, was proposed, and a web framework, a mobile application, and a lightweight authentication algorithm have been implemented to prove this new concept.

The most obvious finding from this study is that the proposed schema reduces inspection costs and decreases the likelihood of potential safety accidents for inspectors. Using drones can reduce equipment rental costs caused by the use of ladders, special inspection vehicles, etc., and can also decrease traffic control costs due to shorter working hours can be reduced. Allowing drones to be used in places where human access is difficult can significantly reduce the work of inspectors at height. This enables inspectors to work more safely. Furthermore, this framework provides intuitive data analysis through the function to manage bridge information including 3D models of bridges and helps to create efficient and easy reports using the collected inspection data. The proposed scheme also provides a platform for sharing data among different parties with an interest, increasing the objectivity of data and allowing connectivity between data. This makes it possible to accumulate big data about bridges. These findings broadly support other research work in this field linking bridge inspections and UAVs.

Another important finding was that the proposed platform improved security compared to the previous research on prototype development. The prototypes have not treated security in much detail, such as not including hashes for passwords. However, the proposed schema is designed by applying the ZT strategy. Threats to each entity were analyzed from the point of view of the CIA, which is the core of security, and appropriate security mediums were applied to the proposed system. A notable improvement is the introduction of the PUF-based algorithm. The algorithm simulated in this framework generates authentication values using only the information that the two objects participating in authentication each know and the values they have produced themselves. The generated values are hashed, and the result is used as the key to encrypt the authentication messages. Even if the message is intercepted during communication, an external intrusion object cannot verify the message. Since this mutual authentication protocol can defend against major cybersecurity attacks including man-in-the-middle attacks, the application of this secure algorithm improved the reliability and safety of the proposed platform.

This research is meaningful in that it proposes a bridge inspection process using UAV and furthermore introduces a 3D bridge model into the inspection web framework. The 3D model is linked with the collected data to enable bridge quality control and facilitate continuous data capture. 3D modeling techniques using UAVs have been proposed, but based on our information, this research is the first approach to introduce a system that integrates a modeling technique with the function of generating bridge inspection reports.

CHAPTER 7: CONCLUSION

Bridge inspections are vital to maintaining the safety of the critical infrastructures that support society. The inspections in West Virginia are performed using visual inspection methods and this traditional approach has cost, safety, and quality issues. Modern UAV technology has given rise to the suggestion that might replace traditional inspection techniques. The objective of this study was to design and implement a reliable platform for Trusted-BIMS replacing current expensive and unsafe manual inspection. The new approach proposed is an interactive bridge inspection schema with built-in security methods while integrating 3D modeling using UAVs into the report generation process. Based on comprehensive research and requirement analysis, a web framework was implemented to share data among various parties with an interest, a mobile application was designed, and a PUF-based algorithm for mutual authentication was adopted. The web system was implemented using PHP as the server-side language, and the mobile application was designed based on React Native. Messages in the mutual authentication algorithm are encrypted using JavaScript on the client-side and PHP on the server-side. MySQL database was used for data management. The suggested procedure was tested in the field to ensure its validity. Experimental results found that using 3D modeling in a UAV-based bridge inspection system reduces the cost and worker safety issues. It also enables the efficient creation and management of inspection reports along with detailed data. It was possible to visually check the overall condition of the bridge through the operation of the 3D models. In addition, the application of security mediums based on threat analysis and device authentication through secure algorithms improved the overall security of the proposed platform. These results broadly support other research work on the UAV-assisted bridge inspection process and the implementation of secure software.

The structural features of the drone used in this research limited imaging under the bridge. There is a possibility that some GPS information will be lost in the process of image extraction from video. In the future, it is recommended to carry out under the traffic control condition when the inspector takes photos of the bottom parts of the bridge. More accurate GPS mapping is suggested when using a moving picture to create 3D models. For the refined implementation of device authentication, research can be carried out on methods to communicate with actual PUF values. Cybersecurity issues may arise for UAVs and various IoT devices involved in the bridge inspection process. It is, therefore, a future research work to investigate more extensive security vulnerabilities and to establish a more comprehensive security scheme. Besides, research on ways to minimize human participation can be proposed. Automatic crack detection can be included in web applications to ensure that data inspection does not require human activity.

In conclusion, this study presented a trusted bridge inspection framework using UAVs. This includes the overall UAV-based bridge inspection process but also a web platform, mobile interface, and mutual authentication using PUF value. It is meaningful in that it creates a 3D model using a UAV and links it with web framework, a bridge inspection reporting module. The findings of this research are expected to be of value to various parties with the same interest in conducting bridge inspections.

CHAPTER 8: FUTURE RESEARCH

Future research can be divided into short-term and long-term improvement. The first short-term improvement is the implementation of a more sophisticated PUF algorithm based on field testing. In this thesis, the PUF value of the IoT device was assigned as an arbitrable number to simulate the security algorithm. Research on the communication method for the actual PUF value included in the System-on-a-Chip (SoC) may be conducted for the implementation of a more complete security algorithm. Second, cybersecurity issues of UAVs and IoT devices are constantly being raised. Future research may suggest identifying more in-depth security vulnerabilities and designing additional security schemes. Examples include MFA and a strong password policy with force reset functions. Third, research on various methods to generate more accurate bridge models is considered. One of the limitations found in the initial field testing for collecting 3D bridge data was the limited imaging under the bridge. This is related to the angle of view issue of the UAV used in the testing. The camera of the drone used was only located in the front part and did not exist above the machine. These structural features made it difficult for the drone to photograph the top of the UAV as it passed under the bridge. Future researchers could address this issue by using machines with a 360-degree field of view or developing customized UAVs. Another limitation was that the field testing conducted without traffic control created constraints in photographing the target bridge due to manned vehicles. This can be improved by performing traffic control during the flight of the drone. Furthermore, there is a possibility that GPS information will be lost in the process of extracting the video into images. This is a factor that lowers the GPS mapping accuracy of the 3D model and the actual captured image. A proposal for a more accurate GPS mapping system is required.

In long-term improvement, research on security responses to unusual access/behavior based on physical location detection using machine learning can be suggested. The research can be extended to implement a more secure schema by improving the safety of the entities involved in the inspection process, and various security technologies can be utilized more widely in the process. Moreover, further studies can be conducted on how to minimize human involvement throughout the bridge inspection process. Research on an automatic crack detecting system using artificial intelligence to decrease human activity is one example. This can be a way to increase the overall efficiency of a bridge inspection.

REFERENCES

Aloft. (n.d.). *B4UFLY*. Retrieved from https://b4ufly.aloft.ai/

Aman, M. N., Chua, K. C., & Sikdar, B. (2017). Mutual authentication in IOT systems using physical unclonable functions. *IEEE Internet of Things Journal, 4*(5), 1327-1340.

American Road and Transportation Builders Association. (2022). *ARTBA bridge report.* Retrieved October 25, 2021, from https://artbabridgereport.org/state/profile/WV

Burgett, J. M., Bausman, D. C., & Commert, G. (2019). *Unmanned aircraft systems (UAS) impact on operational efficiency and connectivity*. Columbia: SC Department of Transportation.

Cybersecurity and Infrastructure Security Agency CISA. (2019, June 11). *Cybersecurity best practices for operating commercial unmanned aircraft systems*. Retrieved October 27, 2021, from https://www.cisa.gov/publication/cybersecurity-best-practices-operating-commercial-unmanned-aircraft-systems

Cybersecurity and Infrastructure Security Agency CISA. (2020, October 21). *Critical infrastructure sectors*. Retrieved October 25, 2021, from https://www.cisa.gov/critical-infrastructure-sectors

Federal Aviation Administration. (2021a, August 30). *Airspace 101 – Rules of the sky*. Retrieved from https://www.faa.gov/uas/getting_started/where_can_i_fly/airspace_101

Federal Aviation Administration. (2021b, June 29). *Certificated remote pilots including commercial operators*. Retrieved from https://www.faa.gov/uas/commercial_operators/

Federal Aviation Administration. (2021c, March 03). *Educational users*. Retrieved from https://www.faa.gov/uas/educational_users/

Federal Aviation Administration. (2021d, October 13). *How to register your drone*. Retrieved from https://www.faa.gov/uas/getting_started/register_drone/

Federal Aviation Administration. (2021e, April 16). *Public safety and government*. Retrieved from https://www.faa.gov/uas/public_safety_gov/

Federal Aviation Administration. (2022, January 05). *Recreational flyers & modeler community-based organizations*. Retrieved from https://www.faa.gov/uas/recreational_fliers/

Federal Highway Administration. (2021). *Collection of data with unmanned aerial systems (UAS) for bridge inspection and construction inspection*. Washington, DC.

Georgia Department of Transportation. (2019). *Field test based guidelines development for the integration of unmanned aerial systems (UASs) in GDOT operations*. Forest Park: Georgia Department of Transportation.

Joint DISA/NSA Zero Trust Engineering Team. (2021, February). *Department of Defense (DOD) Zero trust reference architecture.* Retrieved from https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

Kirk, R. S., & Mallett, W. J. (2018). *Highway bridge conditions: issues for congress.* Congressional Research Service.

Leonard, K. (2015, November 11). *Bridge inspections necessary for long term planning*. (HR Green) Retrieved October 25, 2021, from https://www.hrgreen.com/articles/bridge-inspections-necessary-for-long-term-planning/

Leshko, B. (2015, January 6). *Proposed AASHTO guidelines for complex bridge inspection.* Retrieved October 25, 2021, from https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=3385

Li, Y., & Pu, C. (2020). Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack. *2020 IEEE 23rd International Conference on Computational Science and Engineering (CSE)* (pp. 92-97). Guangzhou: IEEE.

Lovelace, B., & Wells, J. (2018a). Full coverage. *Roads & Bridges, 56*(7), pp. 34-38.

Lovelace, B., & Wells, J. (2018b). *Improving the quality of bridge inspections using unmanned aircraft systems (UAS).* Minnesota Department of Transportation (MnDOT). St. Paul, MS: Research Services & Library.

Lovelace, B., & Zink, J. (2015). *Unmanned aerial vehicle bridge inspection demonstration project.* St. Paul, MN: Minnesota Department of Transportation, Research Services & Library.

Madden, R. L. (1983, June 29). How bridges are inspected and what is being done to make them safer. *The New York Times*, p. 2.

Mao, W., & Boyd, C. (1993). Towards formal analysis of security protocols. *Proceedings Computer Security Foundations Workshop VI*, (pp. 147-158). Franconia.

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations.* National Institute of Standards and Technology, U.S. Department of Commerce.

National Security Agency. (2021, February). *Cybersecurity information sheet: embracing a zero trust security model.* Retrieved from https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

NJDOT Bureau of Research. (2022, July 13). *Integrating UAS in NJ transportation operations*. Retrieved from NJDOT Technology Transfer: https://www.njdottechtransfer.net/uas/

ORACLE. (2022). *11.7 Data type storage requirements*. Retrieved from https://dev.mysql.com/doc/refman/8.0/en/storage-requirements.html#data-types-storage-reqs-strings

Pennsylvania Department of Transportation. (2021). *Bridge safety inspection manual.* Retrieved from https://www.dot.state.pa.us/public/PubsForms/Publications/PUB%20238.pdf

Pu, C., & Li, Y. (2020). Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. *2020 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN).* IEEE.

Pu, C., Wall, A., Ahmed, I., & Choo, K.-K. R. (2022). SecureIoD: A secure data collection and storage mechanism for internet of drones. *2022 23rd IEEE International Conference on Mobile Data Management (MDM)* (pp. 83-92). Paphos: IEEE.

Pu, C., Wall, A., Choo, K.-K. R., Ahmed, I., & Lim, S. (2022). A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment. *IEEE Internet of Things Journal (Impact Factor: 9.471), 9*(12), 9918-9933.

ROAD&BRIDGES. (2016, August 17). *BRIDGE INSPECTION: Ohio Turnpike Commission to test bridge inspections with drones*. Retrieved from ROAD&BRIDGES: https://www.roadsbridges.com/bridges/bridge-inspection/news/10648854/bridge-inspection-ohio-turnpike-commission-to-test-bridge-inspections-with-drones

ROAD&BRIDGES. (2021, March 1). *North Carolina DOT conducts first bridge inspection using drone*. Retrieved from ROAD&BRIDGES: https://www.roadsbridges.com/uav/news/10653773/north-carolina-dot-conducts-first-bridge-inspection-using-drone

ROADS&BRIDGES. (2020, November 6). *Kansas DOT demonstrates disaster response, inspections using drones*. Retrieved from ROADS&BRIDGES: https://www.roadsbridges.com/uav/news/10653414/kansas-dot-demonstrates-disaster-response-inspections-using-drones

Ross, R., McEvilley, M., & Oren, J. (2016). *Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems*. NIST, U.S. Department of Commerce.

Seo, J., Wacker, J. P., & Duque, L. (2018). *Evaluating the use of drones for timber bridge inspection.* Madison: U.S. Department of Agriculture, Forest Service, Forest Products Laboratory.

Song, H., Yoo, W., & Zatar, W. (2022). Interactive bridge inspection research using drone. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1002-1005). Torino: IEEE.

The American Association of State Highway and Transportation Officials (AASHTO). (2019, May 24). *AASHTO survey finds drone use exploding among state DOTs*. (AASHTO Journal) Retrieved October 25, 2021, from https://aashtojournal.org/2019/05/24/aashto-survey-finds-drone-use-exploding-among-state-dots/

The Committee on National Security Systems. (2015). *CNSSI 4009 Committee on National Security Systems (CNSS) glossary.* Retrieved from https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

The Western Transportation Knowledge Network (WTKN). (2018, April 9). *Unmanned aerial vehicles and systems: State surveys and domestic scans.* Retrieved October 25, 2021, from https://transportation.libguides.com/uav/surveys

U.S. Department of Homeland Security. (2009). *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Retrieved from https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2009-508.pdf

U.S. Department of Transportation Federal Highway Administration. (1995). *Recording and coding guide - federal highway administration.*

U.S. Department of Transportation Federal Highway Administration. (2021, June 15). *Bridge condition by highway system 2021*. Retrieved June 16, 2022, from https://www.fhwa.dot.gov/bridge/nbi/no10/condition21.cfm

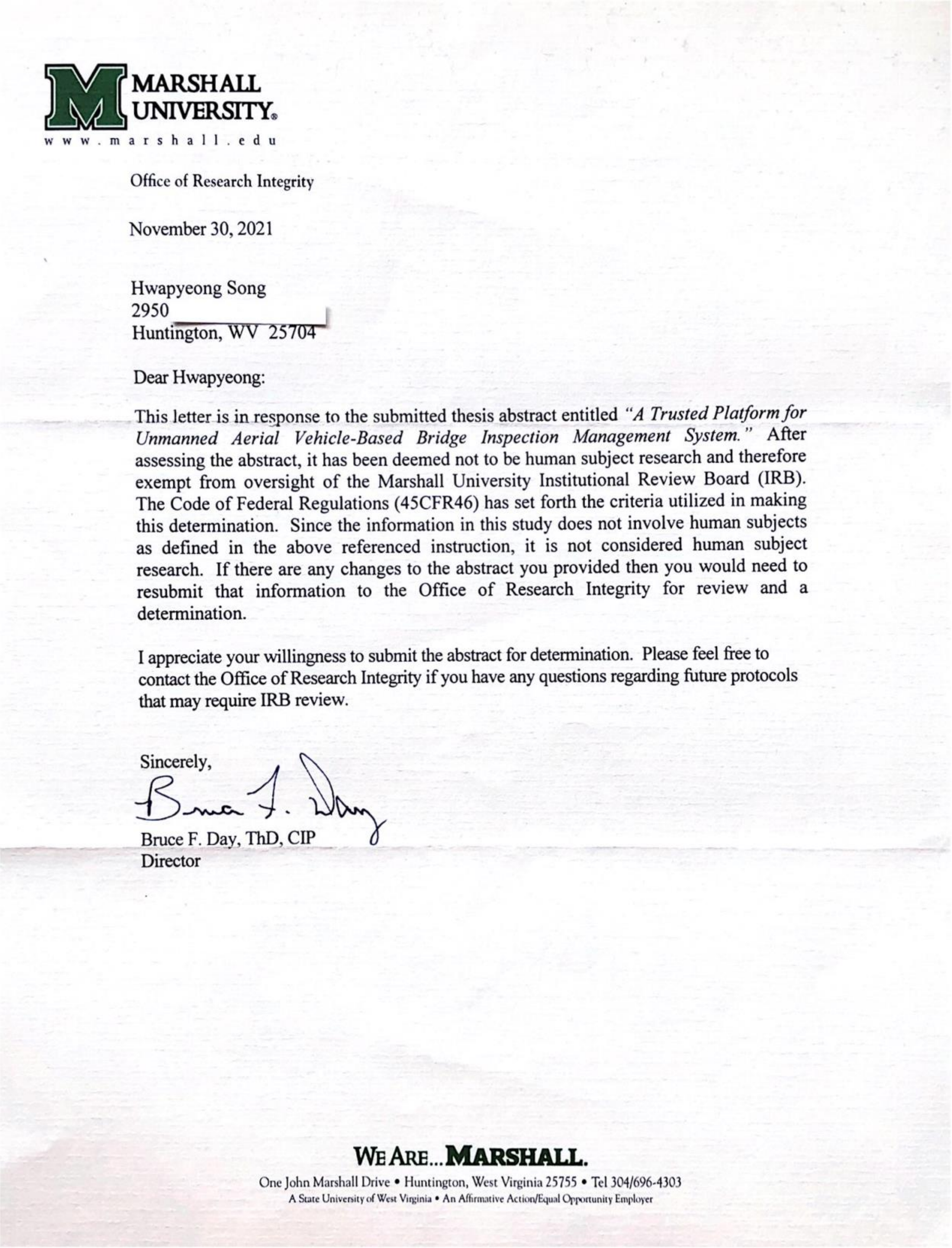
United States Department of Transportation, Bureau of Transportation Statistics. (2022, July 1). *Unmanned aerial vehicles and systems: projects pilots and news*. Retrieved from National Transportation Library: https://transportation.libguides.com/uav/projects

United States Naval Academy. (n.d.). *Information assurance*. Retrieved 07 01, 2022, from https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21/lec.html

Zhang, Y., He, D., Li, L., & Chen, B. (2020). A lightweight authentication and key agreement scheme for internet of drones. *Computer Communications, 154*, 455-464.

Zink, J. (2016, September 6). Will drones transform bridge inspection? *Roads & Bridges, 54*(9), pp. 40-42.

APPENDIX A: APPROVAL LETTER



MARSHALL UNIVERSITY®
www.marshall.edu

Office of Research Integrity

November 30, 2021

Hwapyeong Song
2950 [redacted]
Huntington, WV 25704

Dear Hwapyeong:

This letter is in response to the submitted thesis abstract entitled *"A Trusted Platform for Unmanned Aerial Vehicle-Based Bridge Inspection Management System."* After assessing the abstract, it has been deemed not to be human subject research and therefore exempt from oversight of the Marshall University Institutional Review Board (IRB). The Code of Federal Regulations (45CFR46) has set forth the criteria utilized in making this determination. Since the information in this study does not involve human subjects as defined in the above referenced instruction, it is not considered human subject research. If there are any changes to the abstract you provided then you would need to resubmit that information to the Office of Research Integrity for review and a determination.

I appreciate your willingness to submit the abstract for determination. Please feel free to contact the Office of Research Integrity if you have any questions regarding future protocols that may require IRB review.

Sincerely,

Bruce F. Day

Bruce F. Day, ThD, CIP
Director

WE ARE...MARSHALL.

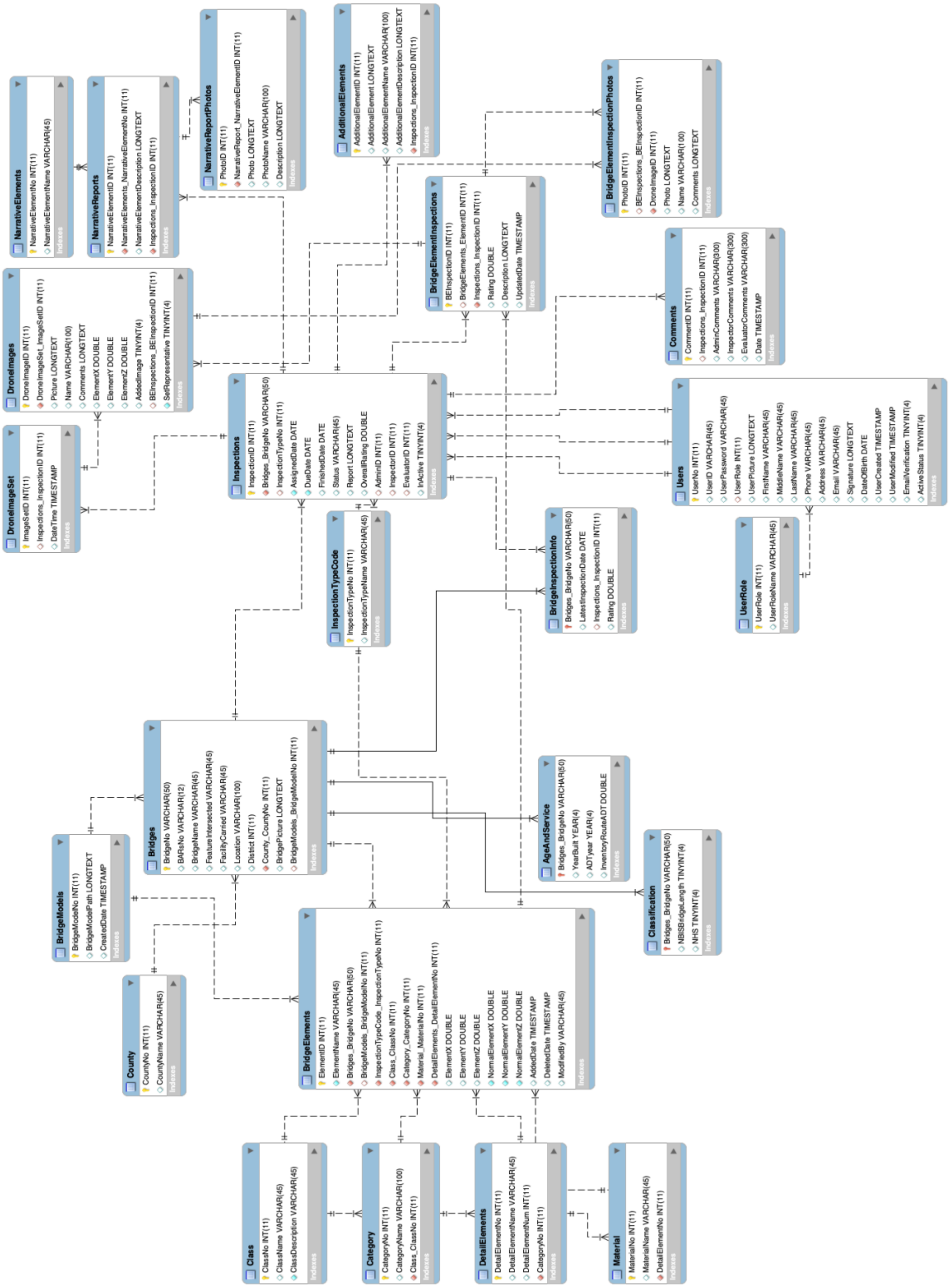
One John Marshall Drive • Huntington, West Virginia 25755 • Tel 304/696-4303
A State University of West Virginia • An Affirmative Action/Equal Opportunity Employer

APPENDIX B: ACRONYMS

3NF	Third Normal Form
AES	Advanced Encryption Standard
BARS	Bridge Analysis and Rating Systems
CBC	Cipher Block Chaining
CCTVs	Closed-Circuit Televisions
CFR	Code of Federal Regulations
CISA	Cybersecurity and Infrastructure Security Agency
CNSS	Committee on National Security Systems
COA	Certificate of Authorization
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
ERD	Entity Relationship Diagram
FAA	Federal Aviation Administration
iBIRD	interactive Bridge Inspection Research using Drone
IoT	Internet of Thing
MDOT	Michigan Department of Transportation
MFA	Multi-Factor Authentication
NBIS	National Bridge Inspection Standards
NSA	National Security Agency
OTP	One-Time Passwords
PennDOT	Pennsylvania Department of Transportation
PUF	Physical Unclonable Function
SHA	Secure Hash Algorithm
SoC	System-on-a-Chip
SQL	Structured Query Language
Trusted-BIMS	Trusted Platform for Bridge Inspection Management System
TRUST	The Recreational UAS Safety Test
UAV	Unmanned Aerial Vehicle
ZT	Zero-Trust

APPENDIX C: DATABASE AND STORED PROCEDURES

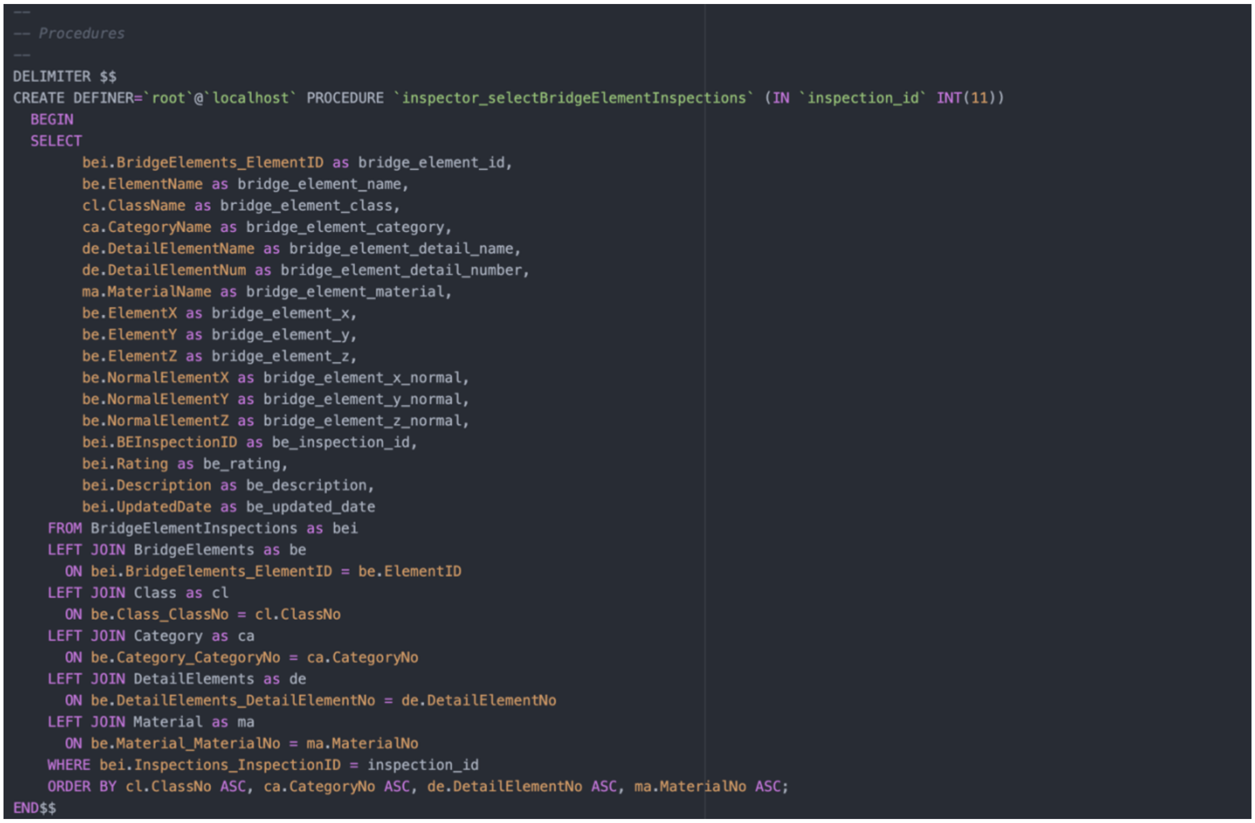
Entity Relationship Diagram (ERD)



Stored Procedure

A stored procedure is a method that stores a series of Structured Query Language (SQL) in the database server in advance and executes a query by a call from a client. In this way, data integrity can be ensured by making it difficult to guess, infer, or manipulate the query statement on the client-side. It can also be used by multiple programs connected to the database via a simple call, allowing code reuse.

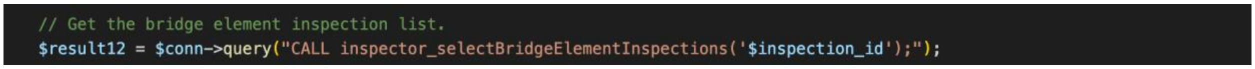
Considering these advantages, the proposed schema adopts stored procedures. The figure below is one example of the applied stored procedures. This procedure is used to get bridge elements for an inspection, and this was tested on a local machine.



```sql
--
-- Procedures
--
DELIMITER $$
CREATE DEFINER=`root`@`localhost` PROCEDURE `inspector_selectBridgeElementInspections` (IN `inspection_id` INT(11))
  BEGIN
  SELECT
        bei.BridgeElements_ElementID as bridge_element_id,
        be.ElementName as bridge_element_name,
        cl.ClassName as bridge_element_class,
        ca.CategoryName as bridge_element_category,
        de.DetailElementName as bridge_element_detail_name,
        de.DetailElementNum as bridge_element_detail_number,
        ma.MaterialName as bridge_element_material,
        be.ElementX as bridge_element_x,
        be.ElementY as bridge_element_y,
        be.ElementZ as bridge_element_z,
        be.NormalElementX as bridge_element_x_normal,
        be.NormalElementY as bridge_element_y_normal,
        be.NormalElementZ as bridge_element_z_normal,
        bei.BEInspectionID as be_inspection_id,
        bei.Rating as be_rating,
        bei.Description as be_description,
        bei.UpdatedDate as be_updated_date
    FROM BridgeElementInspections as bei
    LEFT JOIN BridgeElements as be
      ON bei.BridgeElements_ElementID = be.ElementID
    LEFT JOIN Class as cl
      ON be.Class_ClassNo = cl.ClassNo
    LEFT JOIN Category as ca
      ON be.Category_CategoryNo = ca.CategoryNo
    LEFT JOIN DetailElements as de
      ON be.DetailElements_DetailElementNo = de.DetailElementNo
    LEFT JOIN Material as ma
      ON be.Material_MaterialNo = ma.MaterialNo
    WHERE bei.Inspections_InspectionID = inspection_id
    ORDER BY cl.ClassNo ASC, ca.CategoryNo ASC, de.DetailElementNo ASC, ma.MaterialNo ASC;
END$$
```

Figure 1. Stored Procedure: Server-side

The name of this procedure is 'inspector_selectBridgeElementInspections'. This is used to obtain data on the bridge elements required for each inspection. This procedure receives the inspection ID as a parameter and returns data about the bridge elements included in the inspection. This query is stored on the database server.



```
// Get the bridge element inspection list.
$result12 = $conn->query("CALL inspector_selectBridgeElementInspections('$inspection_id');");
```

Figure 2. Stored Procedure: Client-side

The client calls using the procedure name with a parameter. Because only the procedure's name is shown on the client-side, not the entire query, this simplifies the program code and makes it difficult for malicious users to guess or manipulate the query. As such, the proposed schema maintains data integrity through the use of stored procedures.