

# An Adaptive Encryption-as-a-Service Construction Based on Fog Computing

UNDER THE GUIDANCE  
OF  
Mr. A. RAJKUMAR

PRESENTED BY:  
SIRLA THANVI YADAV-19831A1245  
THALLA YUGANDHAR-19831A1249  
KILARI ESHWAR REDDY-19831A1225

# ABSTRACT

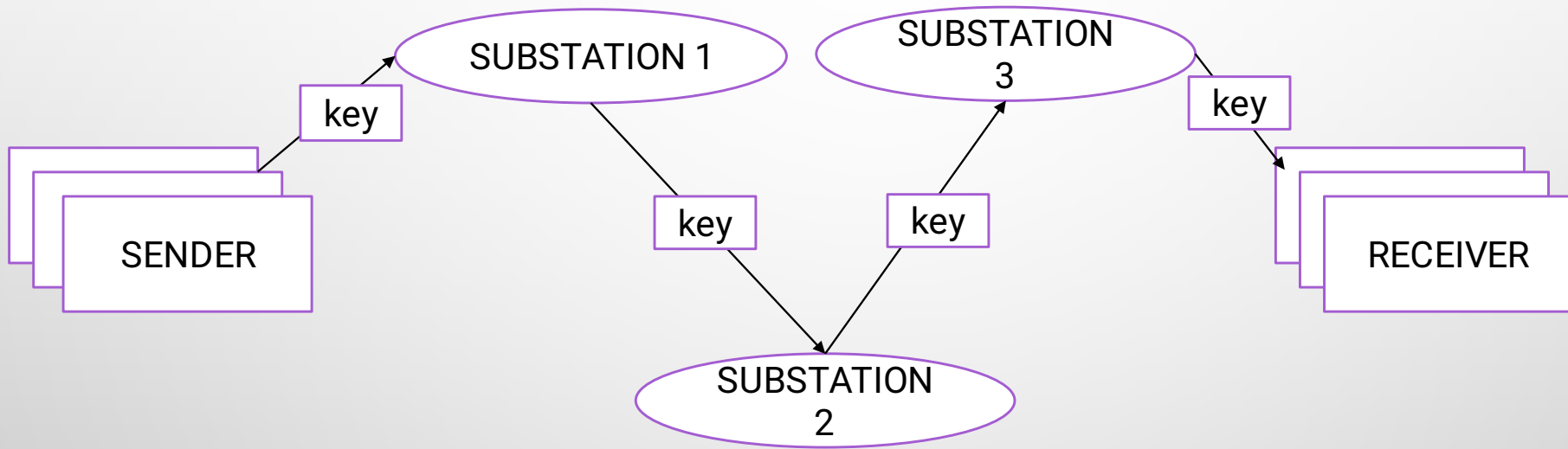
- THE RECENT OUTBREAK OF INDUSTRIAL CYBER ATTACKS INDICATES THAT THE CURRENT INDUSTRIAL NETWORK SECURITY ARCHITECTURE IS UNDER SERIOUS CHALLENGES. AS ONE OF THE CRITICAL INDUSTRIAL NETWORKS, THE HETEROGENEOUS AND REAL-TIME SUBSTATION NETWORK LACKS COMPATIBILITY WITH THE CONVENTIONAL CRYPTOGRAPHY ARCHITECTURE REPRESENTED BY SSL/TLS AND PKI. TO ENHANCE THE SECURITY OF SMART SUBSTATIONS UNDER THE PREMISE OF LOW LATENCY, WE PRESENT A NOVEL ENCRYPTION-AS-A-SERVICE ARCHITECTURE BASED ON FOG COMPUTING IN THIS PROJECT. THE ARCHITECTURE OFFLOADS ENCRYPTION TO DEDICATED DEVICES AND MAKES CERTIFICATE AND KEY MANAGEMENT AVAILABLE THROUGH UNIFIED WEB SERVICES ON THE FOG AND CLOUD LAYERS. BASED ON THIS ARCHITECTURE, WE PROPOSE MX-SORTS, MAXIMIZING SECURITY ON REAL-TIME COMMUNICATION OF DIFFERENT SERVICES, AN ALGORITHM FOR ADAPTIVE CONFIGURATION OF ENCRYPTING AND DECREASING SUBSTATION NETWORK TRAFFIC. BY THE CONTRAST EXPERIMENTS WITH THE CONVENTIONAL CRYPTOGRAPHY ARCHITECTURE, WE PROVE THAT THE ENCRYPTION-AS-A-SERVICE ARCHITECTURE CAN SIGNIFICANTLY IMPROVE THE REAL-TIME AND SECURITY PERFORMANCE OF SUBSTATION NETWORKS.

# PROBLEM IDENTIFICATION

- THE LARGE-SCALE AND RAPIDLY GROWING GRID NETWORK SECURITY INCIDENTS INDICATE THAT THE CURRENT NETWORK SECURITY ARCHITECTURE OF POWER GRIDS, ESPECIALLY THAT OF THE SMART SUBSTATION, REQUIRES A REFORM RATHER THAN MERE SECURITY PATCHES OR GUIDELINES. CRYPTOGRAPHY IS AN IMPORTANT MEANS OF COMBATING THESE SECURITY ISSUES. HOWEVER, THE DEPLOYMENT OF CRYPTOGRAPHY FACILITIES IN SUBSTATION NETWORKS IS FACING CHALLENGES . BASED ON THIS ARCHITECTURE, WE PROPOSE MX-SORTS, MAXIMIZING SECURITY ON REAL-TIME COMMUNICATION OF DIFFERENT SERVICES, AN ALGORITHM FOR ADAPTIVE CONFIGURATION OF ENCRYPTING AND SIGNING SUBSTATION NETWORK TRAFFIC. BY THE CONTRAST EXPERIMENTS WITH THE CONVENTIONAL CRYPTOGRAPHY ARCHITECTURE, WE PROVE THAT THE ENCRYPTION-AS-A-SERVICE ARCHITECTURE CAN SIGNIFICANTLY IMPROVE THE REAL-TIME AND SECURITY PERFORMANCE OF SUBSTATION NETWORKS.

# EXISTING SYSTEM

- THE LARGE-SCALE AND RAPIDLY GROWING GRID NETWORK SECURITY INCIDENTS INDICATE THAT THE CURRENT NETWORK SECURITY ARCHITECTURE OF POWER GRIDS, ESPECIALLY THAT OF THE SMART SUBSTATION, REQUIRES A REFORM RATHER THAN MERE SECURITY PATCHES OR GUIDELINES. CRYPTOGRAPHY IS AN IMPORTANT MEANS OF COMBATING THESE SECURITY ISSUES.
- HOWEVER, THE DEPLOYMENT OF CRYPTOGRAPHY FACILITIES IN SUBSTATION NETWORKS IS FACING CHALLENGES.
- *EXISTING ALGORITHM*
- TRADITIONAL CRYPTOGRAPHIC TECHNIQUES



# DRAWBACKS OF EXISTING SYSTEM

- IN EXISTING SYSTEM IN SPITE OF THE GATEWAY FIREWALL AND THE VPN, THE SUBSTATION NETWORK IS STILL EXPOSED TO VARIOUS ATTACKS.
- THERE IS A CHANCE OF TRAFFIC FORGERY, TAMPERING AND EAVESDROPPING, WHICH CAN BE MITIGATED BY ENCRYPTION AND AUTHENTICATION OF THE NETWORK TRAFFIC.
- UNAUTHORIZED OPERATIONS OF OPERATORS OR MAINTAINERS ALSO CONTRIBUTE A LOT TO THE DATA LEAKAGE.

# PROPOSED SYSTEM AND ALGORITHM

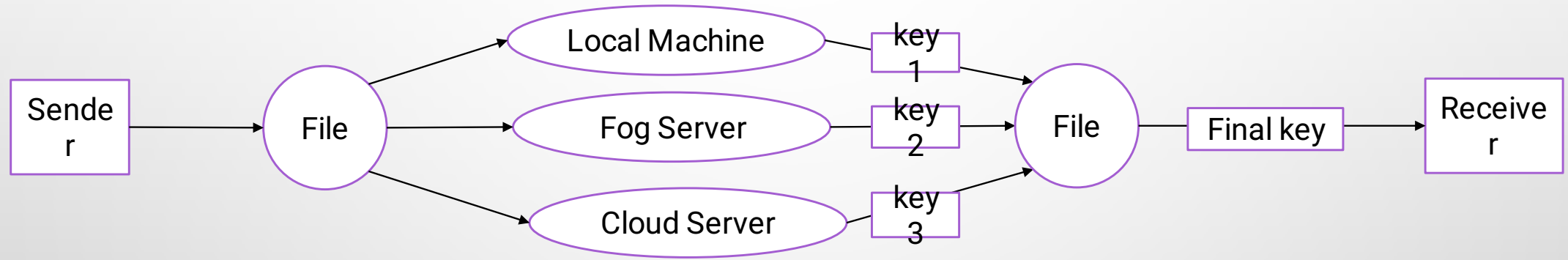
IN THIS PROJECT, WE PROPOSE A HIERARCHICAL ENCRYPTION-AS-A-SERVICE ARCHITECTURE BASED ON FOG COMPUTING AND MX-SORTS ALGORITHM FOR ADAPTIVE CRYPTOGRAPHY CONFIGURATIONS IN THE REAL TIME COMMUNICATION OF SMART SUBSTATIONS.

➤ WE PRESENT NOVEL FLEXIBLE CRYPTOGRAPHY ARCHITECTURE THROUGH THE DECOUPLING OF ENCRYPTION AND BUSINESS PROCESSES.

➤ OUR PROPOSED SYSTEM ENSURES THE REAL-TIME PERFORMANCE AND EXTENSIBILITY OF THE ENCRYPTION-AS-SERVICE ARCHITECTURE.

MX-SORTS: MAXIMIZING SECURITY ON REAL-TIME COMMUNICATION OF DIFFERENT SERVICES.

## BLOCK DIAGRAM:





# ADVANTAGES OF PROPOSED SYSTEM

- OUR PROPOSED SYSTEM ARCHITECTURE CAN SIGNIFICANTLY IMPROVE THE REAL-TIME AND SECURITY PERFORMANCE OF SUBSTATION NETWORKS.
- MX-SORTS ALGO MAXIMIZE THE SECURITY UNDER THE PREMISE OF REAL-TIME ASSURANCE IN SUBSTATION COMMUNICATIONS.

# HARDWARE REQUIREMENTS

- PROCESSOR : DUAL CORE 2 DUO.
- RAM : 2GB DD RAM
- HARD DISK : 250 GB

# SOFTWARE REQUIREMENTS

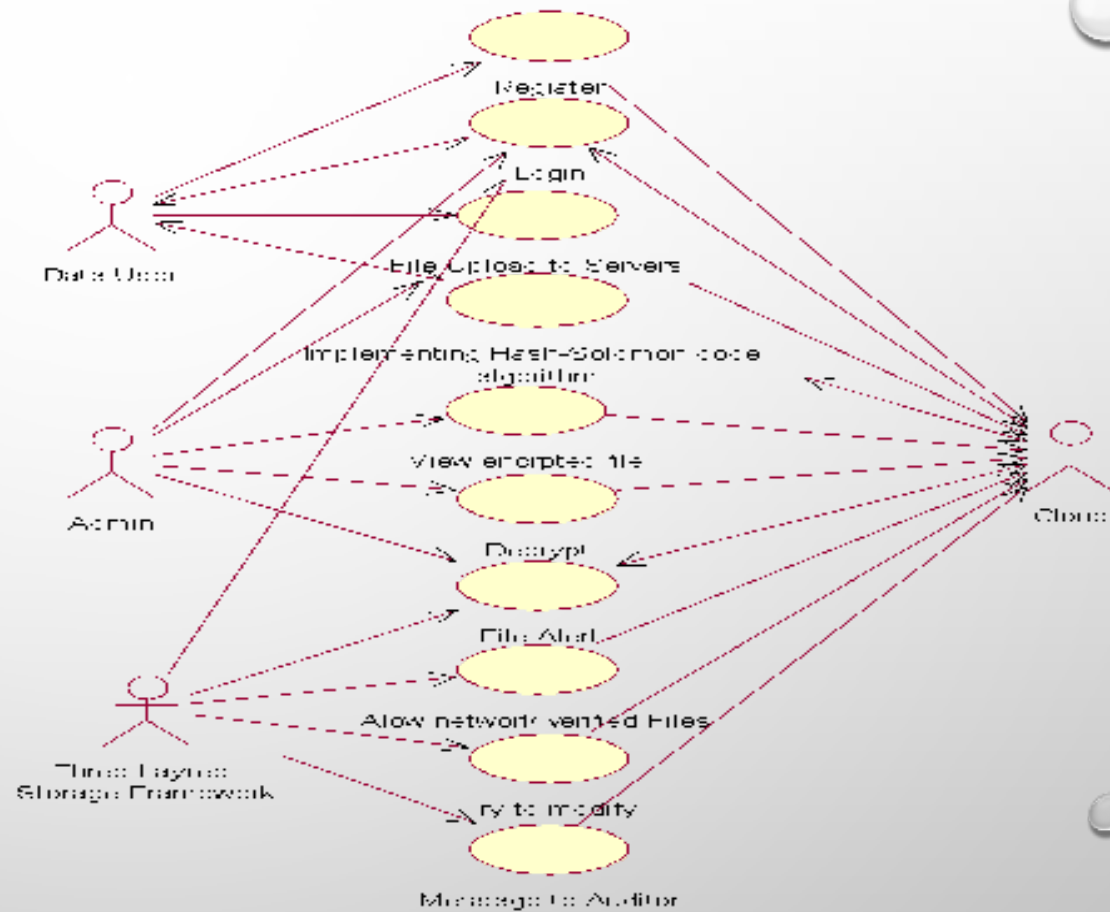
- FRONT END : J2EE (JSP, SERVLET)
- BACK END : MY SQL 5.5
- OPERATING SYSTEM : WINDOWS 7
- IDE : ECLIPSE

# LITERATURE SURVEY

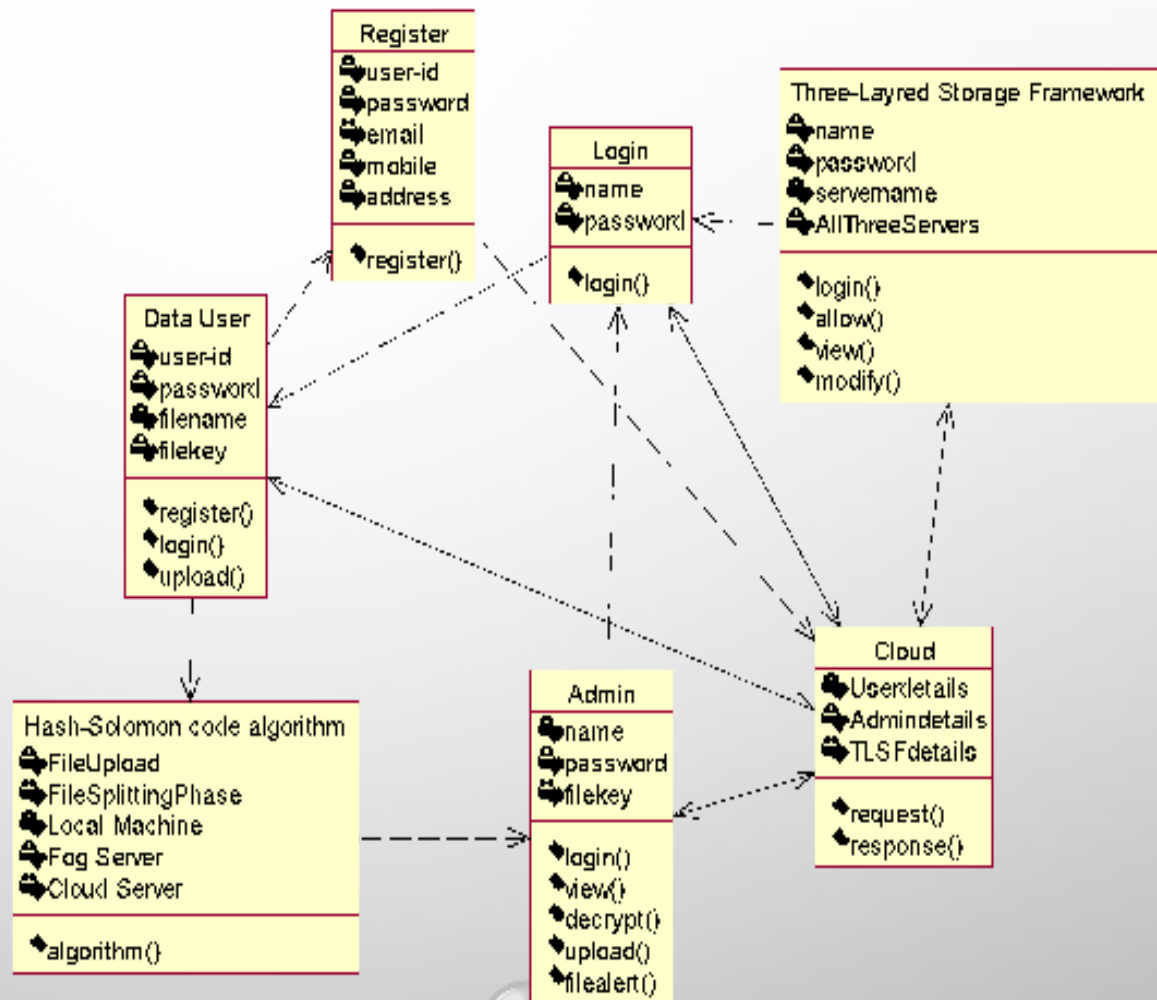
- TITLE: PRO-RUSSIAN HACKERS CLAIM RESPONSIBILITY FOR KNOCKING U.S. AIRPORT WEBSITES
- AUTHOR: VANESSA ROMO
- YEAR: 2022, OCT 10
- DESCRIPTION:

PRO-RUSSIAN HACKER GROUP IS TAKING CREDIT FOR TEMPORARILY TAKING DOWN SEVERAL U.S. AIRPORT WEBSITES ON MONDAY, THOUGH THERE APPEARED TO BE NO IMPACT ON FLIGHT OPERATIONS. THE CYBERATTACKS CLAIMED BY KILLNET IMPACTED THE WEBSITES FOR LOS ANGELES INTERNATIONAL, CHICAGO O'HARE, AND HARTSFIELD-JACKSON INTERNATIONAL IN ATLANTA, AMONG OTHERS. THE GROUP POSTED A LIST OF AIRPORTS ON TELEGRAM, URGING HACKERS TO PARTICIPATE IN WHAT'S KNOWN AS A DDOS ATTACK — A DISTRIBUTED DENIAL-OF-SERVICE CAUSED WHEN A COMPUTER NETWORK IS FLOODED BY SIMULTANEOUS DATA TRANSMISSIONS.

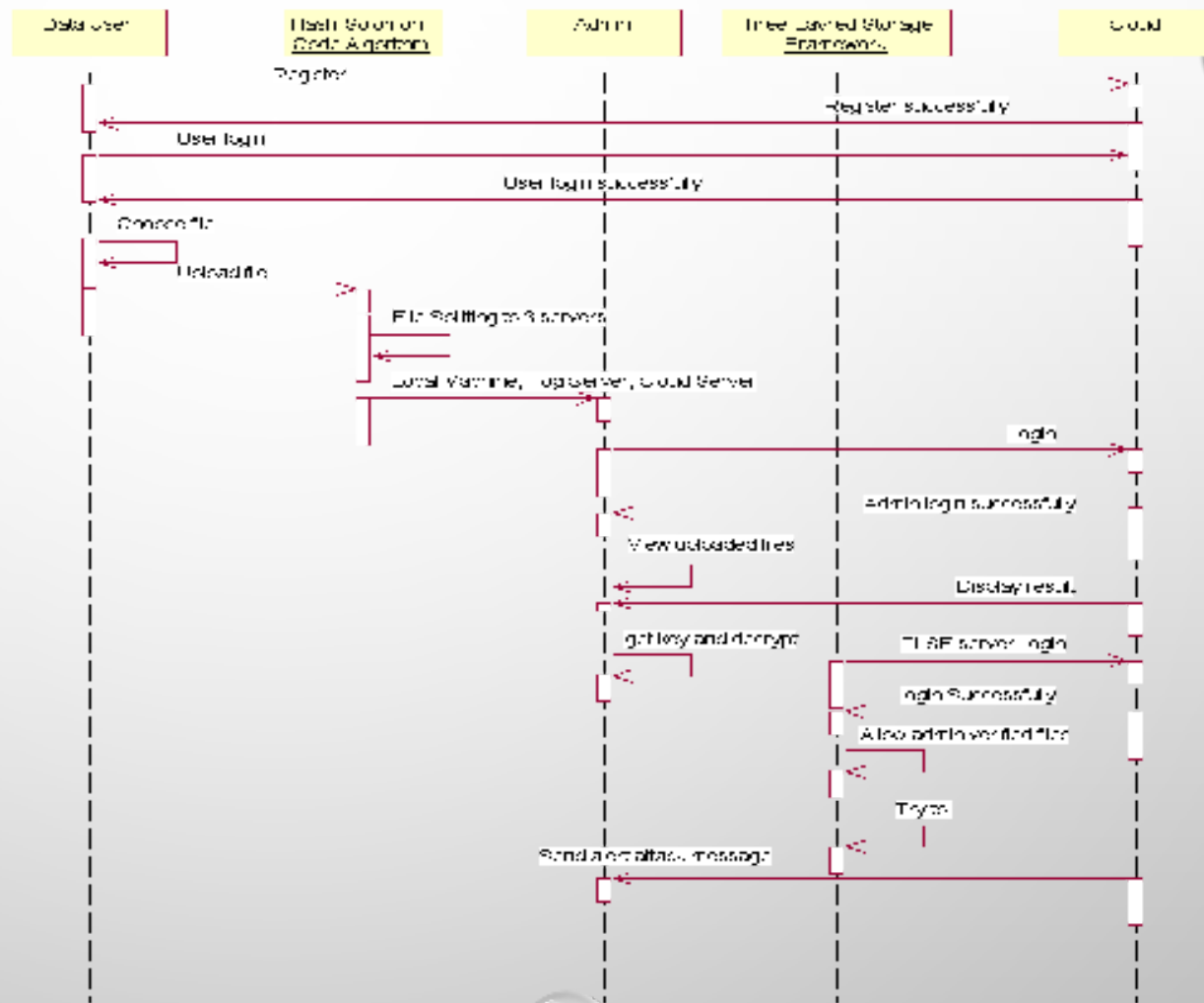
# USE CASE DIAGRAM:



# Class diagram:



# Sequence Diagram:



# SOFTWARE TESTING

## GENERAL

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

## DEVELOPING METHODOLOGIES

The test process is initiated by developing a comprehensive plan to test the general functionality and special features on a variety of platform combinations. Strict quality control procedures are used. The process verifies that the application meets the requirements specified in the system requirements document and is bug free. The following are the considerations used to develop the framework from developing the testing methodologies.

# TYPES OF TESTING

## UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

## FUNCTIONAL TESTING



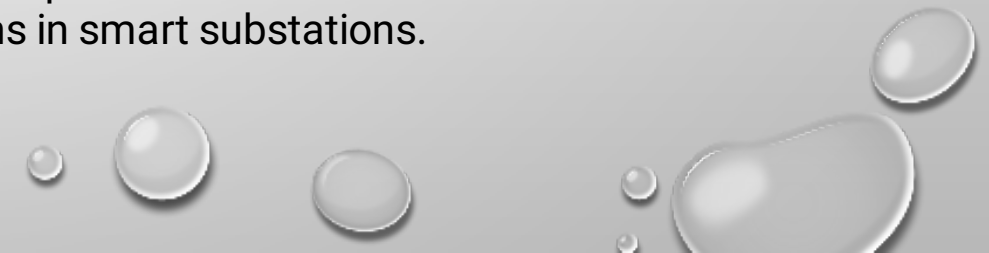


## FUTURE ENHANCEMENTS

In the future, we will deploy our architecture in more industrial control networks, such as sewage treatment factories, which have distinct real-time requirements and communication protocols.

## CONCLUSION

In this paper, we propose the MX-SORTS algorithm to adaptively configure the selection of cryptographic methods on different services, so that we can balance between the delay of the encryption and real-time requirements of substation networks. We introduce the concept of encryption-as-a-service into smart substations and migrate time-consuming key management to the fog node. By integrating the certificate server to RTUs, we can achieve real-time performance in secured communications in smart substations.







The image features a light gray background with a subtle gradient. In the corners, there are several realistic-looking water droplets of various sizes, some with highlights and shadows, giving them a 3D effect. The text "Thank You" is centered in the middle of the image.

Thank You