2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

AN EFFICIENT KEY MANAGEMENT AND MULTI-LAYERED SECURITY FRAMEWORK FOR SCADA SYSTEMS

[1,2,3,4] **Pothala Bhavya, Sapa Mounika, Gande Ramu, Sanjeeth Kumar,**
[5]**K. Krishna**

[1,2,3,4] Ug scholars, MallaReddy college Of Engineering , Hyderabad - 500100

[5] Assistant Professor, MallaReddy college Of Engineering , Hyderabad - 500100

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) networks play a vital role in industrial control systems. Industrial organizations perform operations remotely through SCADA systems to accelerate their processes. However, this enhancement in network capabilities comes at the cost of exposing the systems to cyber-attacks. Consequently, effective solutions are required to secure industrial infrastructure as cyber-attacks on SCADA systems can have severe financial and/or safety implications. Moreover, SCADA field devices are equipped with microcontrollers for processing information and have limited computational power and resources. This makes the deployment of sophisticated security features challenging. As a result, effective lightweight cryptography solutions are needed to strengthen the security of industrial plants against cyber threats.

CHAPTER-1

INTRODUCTION

1.1 INTRODUCTION

There has been a surge in the deployment of Supervisory Control and Data Acquisition (SCADA) systems to control and monitor industrial infrastructure over the Internet. Organizations such as oil and natural gas, power stations, water & sewage systems, chemical plants, manufacturing units, railway, and other transportation use SCADA systems to monitor and control their infrastructure such as oil pipelines, solar panels, water pipelines, boilers, railway tracks, and plant floor components across open access networks.

1.2 OBJECTIVE

SCADA communication messages have sensitive information as they are used to monitor and control the plant floor devices. For example, in water and sewage systems, the communication messages are used to raise and lower water tank levels or open and close the safety valves.

CHAPTER-2

LITERATURE SURVEY

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

2.1 LITERATURE SURVEY

Literature survey 1:

Title: A Vulnerabilities' assessment and mitigation strategies for the small Linux server.

Year: 20210

Author: D. Upadhyay, S. Sampalli, and B. Plourde.

Description: The merger of SCADA (supervisory control and data acquisition) and IoTs (internet of things) technologies allows end-users to monitor and control industrial components remotely. However, this transformation opens up a new set of attack vectors and unpredicted vulnerabilities in SCADA/IoT field devices. Proper identification, assessment, and verification of each SCADA/IoT component through advanced scanning and penetration testing tools in the early stage is a crucial step in risk assessment.

Literature survey 2:

Title: SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations.

Year: 2020

Author: D. Upadhyay and S. Sampalli

Description:

Growing dependency and remote accessibility of automated industrial automation systems have transformed SCADA (Supervisory Control and Data Acquisition) networks from strictly isolated to highly interconnected networks. This increase in interconnectivity between systems raises operational efficiency due to the ease of controlling and monitoring of processes, however, this inevitable transformation also exposes the control system to the outside world. As a result, effective security strategies are required as any vulnerability of the SCADA system could generate severe financial and/or safety implications.

CHAPTER-3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

1.These techniques fall under two main categories, namely, centralized key management and decentralized key management schemes.

2.Moreover, each of these categories uses three approaches to generate and extract the session key, namely, symmetric, asymmetric, and hybrid.

3.2 DRAWBACKS

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

1.In a decentralized approach, the keys are created using keying material and may only affect the single communication link in case of a breakdown.

2.Less Security.

3.3 PROPOSED SYSTEM

1.The proposed work aims to offer a multi-layered security framework for industrial infrastructures by combining both symmetric and asymmetric key cryptography techniques.

2.This novel approach follows a layered architecture, where the MTU and sub-MTU can communicate using a hybrid technique for an entire session while the sub-MTU and RTU can communicate using symmetric key cryptography once the session key is securely exchanged.

3.4 ADVANTAGES

1..A multi-layered framework by combining both symmetric and asymmetric key cryptographic techniques.

2.High security.

3.It's provided authentication and confidentiality.

3.5 SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS

HARDWARE:

- PROCESSOR
  : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.
- RAM
  : 512 MB DD RAM
- MONITOR
  : 15" COLOR
- HARD DISK
  : 40 GB

SOFTWARE REQUIREMENTS

SOFTWARE:

- Front End
  : J2EE (JSP, SERVLET)
- Back End
  : MY SQL 5.5
- Operating System
  : Windows 7
- IDE
  : Eclipse

CHAPTER-4

SYSTEM DESIGN

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

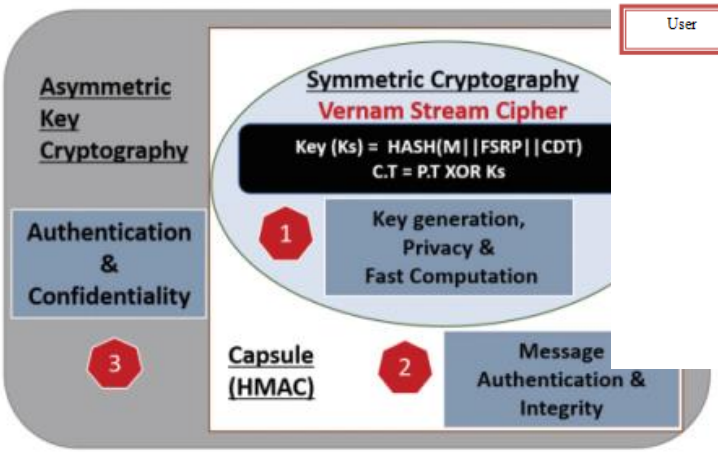


Fig 4.1.1 System Architecture Model

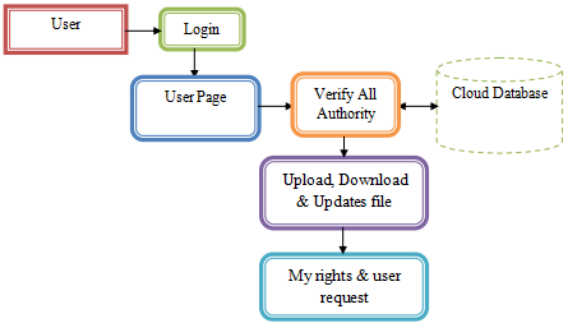


Fig 4.2.2.2 Cloud User

4.2 METHODOLOGIES

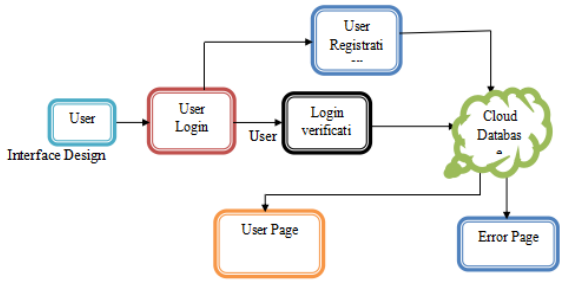
4.2.1 MODULES NAME:

This project having the following 5 modules:

1. User Interface.
2. Cloud User
3. Cloud Authority
4. Admin
5. Deduplicatable dynamic pos

4.2.2 MODULES EXPLANATION AND DIAGRAM

- **User Interface Design**



- **Cloud User**

CHAPTER-5

SYSTEM IMPLEMENTATION

5.1 NETWORK SECURITY

Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

How does network security work?

Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

How do I benefit from network security?

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

5.2 JAVA

This chapter is about the software language and the tools used in the development of the project. The platform used here is JAVA. The Primary languages are JAVA, J2EE and J2ME. In this project J2EE is chosen for implementation.

5.3 THE JAVA FRAMEWORK

Java is a programming language originally developed by James Gosling at Microsystems and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++ but has a simpler object model and fewer low-level facilities. Java applications are typically compiled to byte code that can run on any Java Virtual Machine (JVM) regardless of computer architecture. Java is general-purpose, concurrent, class-based, and object-oriented, and is specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere".

5.4 OBJECTIVES OF JAVA

To see places of Java in Action in our daily life, explore java.com.

Why

Software

Developers

Choose Java

Java has been tested, refined, extended, and proven by a dedicated community. And numbering more than 6.5 million developers, it's the largest and most active on the planet. With its versatility, efficiency, and portability, Java has become invaluable to developers by enabling them to:

SOURCE CODE:

```
<%@page
import="com.oreilly.servlet.*,java.sql.*,java
.lang.*,java.text.SimpleDateFormat,java.util
.*,java.io.*,javax.servlet.*,
javax.servlet.http.*" %>

<%@ page import="java.sql.*"%>
<%@ include file="connect.jsp" %>

<html>
<head>
</head>
<body>
<%

ArrayList list = new ArrayList();
ServletContext context =
getServletContext();

String dirName ="C:/Gallery/";
String paramname=null;
```

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

```
String file=null;
Stringa=null,b=null,c=null,d=null,ee=null,ff
=null,gg=null,hh=null,ii=null,image=null,im
age2=null;

FileInputStream fs=null,fs2=null;

File file1 = null,file2 = null;

try {
MultipartRequest multi = new
MultipartRequest(request, dirName, 10 *
1024 * 1024); // 10MB

Enumeration params =
multi.getParameterNames();
while (params.hasMoreElements())
{
paramname = (String)
params.nextElement();
if(paramname.equalsIgnoreCase("name"))
{
a=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("pwd"))
{b=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("dob"))
{
c=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("email"))
{
d=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("mob"))
{
ee=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("cap"))
{
ff=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("utype"))
{
gg=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("stype"))
{
hh=multi.getParameter(paramname);
}
if(paramname.equalsIgnoreCase("t1"))
{
ii=multi.getParameter(paramname);
}
}
        int f = 0;
                Enumeration files =
multi.getFileNames();
                while
(files.hasMoreElements())
                {
                paramname = (String)
files.nextElement();

                if(paramname != null)
                {
        f = 1;
    image                                   =
multi.getFilesystemName(paramname);
    String fPath = "C:\\Gallery\\"+image;
     file1 = new File(fPath);
        fs = new FileInputStream(file1);
        list.add(fs);

        if (files.hasMoreElements())
        {



        {

        }

           }
         }


            FileInputStream fs1 = null;

              int lyke=0;
                        String
as="Rejected";
```

CHAPTER-6

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

TESTING

6.1 TESTING

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 tests. Each test type addresses a specific testing requirement.

6.2 Types of Tests

6.2.1 Unit Testing

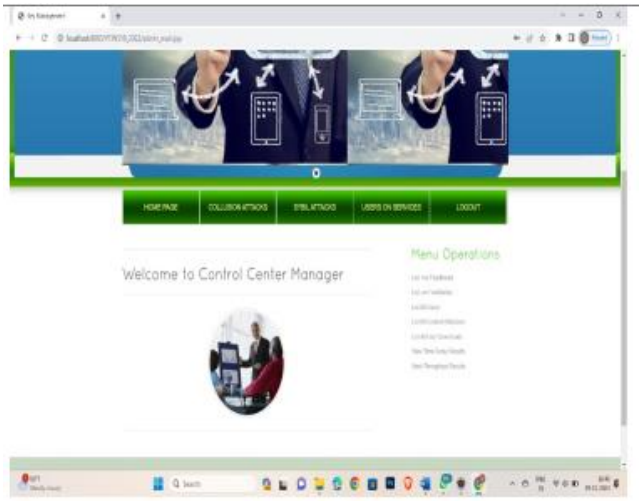
Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is 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.

CHAPTER-7

RESULTS

7.1 SCREENSHOTS

7.1.1 Home page



7.1.2 control center manager

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

7.1.3 Control center login details

7.1.4 User Registration page

CHAPTER-8

CONCLUSION

8.1 CONCLUSION

The protection of critical industrial infrastructure against cyber-attacks is crucial for ensuring public safety, security, and reliability. SCADA system are used to control and monitor such industrial control systems. A robust solution to strengthen the security of these systems against cyber-attacks is a crucial requirement in the design of SCADA systems. Through this work, we aim to cover the protection of the industrial control system landscape by offering a low cost and robust framework for SCADA networks, which protects them against various cyber-attacks. In this paper, we have proposed a session key agreement in addition to lightweight multi-layered encryption techniques. The framework combines both symmetric and asymmetric cryptography to achieve high computational speed by covering all the security mechanisms. This security model is proposed to enhance the security of various industrial sectors such as water and sewage plants, power stations, chemical plants, oil industries, product manufacturing units, and transportation systems. The successful deployment of this model will allow operators and technicians to monitor and control the plant devices remotely as it will protect the entire system from potential breaches.

CHAPTER-9

FUTURE ENHANCEMENTS

9.1 FUTURE ENHANCEMENT

Further, an efficient session key management mechanism is proposed by merging random number generation with a hashed message authentication code. Moreover, for each session, we have introduced three symmetric key cryptography techniques based on the

concept of Vernam cipher and a pre-shared session key, namely, random prime number generator, prime counter, and hash chaining. The proposed scheme satisfies the SCADA requirements of real-time request response mechanism by supporting broadcast, multicast, and point to point communication.

CHAPTER-10

REFERENCES

10.1 REFERENCES:

[1] D. Upadhyay, S. Sampalli and B. Plourde, "Vulnerabilities' assessment and mitigation strategies for the small linux server Onion Omega2", Electronics, vol. 9, no. 6, pp. 967, 2020.

[2] D. Upadhyay and S. Sampalli, "SCADA (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations", Comput. Security, vol. 89, Feb. 2020.

[3] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems", Comput. Security, vol. 56, pp. 1-27, Feb. 2016.

[4] Rezai, P. Keshavarzi and Z. Moravej, "Key management issue in SCADA

networks: A review", Int. J. Eng. Sci. Technol., vol. 20, no. 1, pp. 354-363, 2017.

[5] F. M. Salem, E. Ibrahim and O. Elghandour, "A lightweight authenticated key establishment scheme for secure smart grid communications", Int. J. Safety Security Eng., vol. 10, no. 4, pp. 549-558, 2020.