International Journal of Thesis Projects and Dissertations (IJTPD)
Vol. 3, Issue 1, pp: (100-111), Month: January - March 2015, Available at: www.researchpublish.com

Anomaly Detection and Prevention in Secure Data Transmission

[1]MAYUR KHARADE, [2]ABHIJEET PATIL, [3]VITTHAL KHANDKE, [4]YOGESH NIKUMBH, [5]SAGAR PATIL

Department Of Information Technology, Tssm's Padmabhooshan Vasantdada Patil Institute Of Technology Bavdhan Pune-21, India

Abstract: **There are many techniques in market to send data securely. Data can be sends after applying any specific security check over specific data. But, now a day's problem is to secure data as well as communicate with different platform. Because, some using Windows platform some using UNIX or any other platform. The Main purpose of this project is to transfer data from one end to other securely by applying some defined security check as well as some encryption technique with some crosschecking bits and with some secure protocols (Basic tHTTP, WSHTTP, Net TCP). Now a day's this project are very useful because data transmission is every day activity over internet or personal network via transmission line or physical media or any other way. This project is platform independent. Encryption techniques over internet, Windows Communication Foundation, XHTML, Android are used in this project because of this we can provide cross platform communication which security to provide communication personal and secure to send data between two ends. Re usability of this project is, if we deploy this project then any platform, any person can be use this without much work. Ex. Whatsapp. Maintainability is only with frequently monitoring any update security check for this we were use the Encryption techniques, common format (xml), different data binding techniques (Basic Http, wshttp, Nettcp) etc.we use Extensible Markup Language (XML) is markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in the XML 1.0 Specification produced by the W3C, and several other related specifications, all free open standards. The design goals of XML emphasize simplicity, generality, and usability over the Internet. It is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.**

Keywords: **Basic http, WSHTTP, Net TCP, Data Transmission, Anomaly Detection and Prevention in Secure.**

1. INTRODUCTION

There are many techniques in market to send data securely. Data can be sends after applying any specific security check over specific data. But, now a day's problem is to secure data as well as communicate with different platform. Because, some using Windows platform some using UNIX or any other platform. The Main purpose of this project is to transfer data from one end to other securely by applying some defined security check as well as some encryption technique with some crosschecking bits and with some secure protocols (Basic http, WSHTTP, Net TCP).

1.1. Need:

Misuse detection is the process of detecting and reporting uses of processing systems and networks that would be deemed inappropriate or unauthorized if known to the responsible parties. Even though designers, owners, and administrators of systems and networks usually try to prevent misuses, the complexity of modern system environments and the difficulty of preventing authorized users from abusing their privileges make it virtually impossible to anticipate and prevent all possible security problems. To date, however, there is no known system or method for effectively and independently detecting and reporting misuses and facilitating their subsequent investigation. Processing system misuse detection and reporting research has been funded by U.S. government agencies who have concerns for the confidentiality of their computer systems. Researchers have generally been associated with large research organizations or national laboratories. These institutions have required detailed knowledge of technical computer security, known threats and vulnerabilities, protection mechanisms, standard operational procedures, communications protocols, details of various systems' audit trails, and legal investigation of computer crimes. This misuse detection and reporting research has followed two basic approaches: anomaly detection systems and expert systems, with the overwhelming emphasis on anomaly detection. **1.2.**

1.2 Basic Concept:

A technical outcome of the invention is that it improves on previous misuse detection systems by minimizing the number of false positives. This is achieved by creating signatures from undesirable activities including known attack outcomes, known system vulnerabilities and known attack procedures. Since a misuse is only reported upon a direct match to a known misuse signature, the probability of falsely reporting a misuse is reduced over the previous anomaly detection mechanisms. An additional technical advantage of the invention is that it eliminates the need for expert programming in knowledge-based or rule-based systems. The signatures that the present invention uses are generated by a programmer and are loadable at program initiation. System programmers are capable of creating their own misuse signatures from their particular known attack procedures, attack outcomes, and known system vulnerabilities. Misuse signatures that the present invention uses are deterministic, unlike expert systems. This significantly simplifies development and testing in response to an intrusion or a misuse. A third technical advantage of the invention is that it uses an efficient match and compare method to improve speed. The elimination of the need to maintain statistical histograms, compute statistical deviations, and process rules in a knowledge-based system enables the invention to process data more efficiently, thereby increasing the number of systems whose data can be processed by a single misuse engine.

1.3. Application:

Now a day's this project are very useful because data transmission is every day activity over internet or personal network via transmission line or physical media or any other way. This project is platform independent. Encryption techniques over internet, Windows Communication Foundation, XHTML, Android are used in this project because of This we can provide cross platform communication which security to provide communication personal and secure to send data between two ends. Re usability of this project is, if we deploy this project then any platform, any person can be use this without much work. Ex.

Whatsapp. Maintainability is only with frequently monitoring any update security check for this we were use the Encryption techniques, common format (xml), different data binding techniques (Basic Http, wshttp, Nettcp) etc.we use Extensible Markup Language (XML) is markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in the XML 1.0 Specification produced by the W3C, and several other related specifications, all free open standards. The design goals of XML emphasize simplicity, generality, and usability over the Internet. It is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.

2. LITERATURE SURVEY

2.1. Related work done:

In December 2008, a group of researchers used this technique to fake SSL certificate validity and CMU Software Engineering Institute now says that MD5 should considered cryptographically broken and unsuitable for further use", and most U.S. government applications now require theSHA-2 family of hash functions. In 2012, the Flame malware exploited the weaknesses in MD5 to fake a Microsoft digital signature. The Main purpose of this project is to transfer data from one end to other securely by applying some defined security check as well as some encryption technique with some crosschecking bits and with some secure protocols like The MD5 message-digest algorithm, WsHttp Binding technique, Windows Communication Foundation (WCF).

Processing system misuse detection and reporting research has been funded by U.S. government agencies who have concerns for the confidentiality of their computer systems. Researchers have generally been associated with large research organizations or national laboratories. These institutions have required detailed knowledge of technical computer security, known threats and vulnerabilities, protection mechanisms, standard operational procedures, communications protocols, details of various systems' audit trails, and legal investigation of computer crimes. This misuse detection and reporting research has followed two basic approaches: anomaly detection systems and expert systems, with the overwhelming emphasis on anomaly detection.

2.2. Existing System:

According to our project, provides a method and system for detecting intrusion and misuse of data processing systems that overcomes limitations associated with known detection methods and systems. The present invention provides a method and system for intrusion and misuse detection that minimizes the number of false positive misuse reports eliminates the need for expert system programmers to enter knowledge database rules in a system, and permits rapid processing of data from multiple systems using a single computer. According to one aspect of the invention, there is provided an intrusion misuse detection and reporting system that uses processing system inputs, which include processing system audit trail records, system log file data, and system security state data information for further analysis to detect and report processing system intrusions and misuses. A misuse selection mechanism allows the detection system to analyze the process inputs for a selected subset of misuses. The processing system inputs are then converted into states which are compared, through the misuse engine, to a predefined set of states and transitions until a selected misuse is detected. Once a misuse has been detected, an output mechanism generates a signal for use by notification and storage mechanism. The detection system then generates a text-based output report for a user to view or store.

3. PROJECT STATEMENT

3.1. PROBLEM STATEMEN:

To implement Anomaly detection and prevention in secure data transmission over web.

3.2. Technology Used:

Extensible Markup Language (XML) is markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine- readable. It is defined in the XML 1.0 Specification produced by theW3C, and several other related specifications, all free open standards.

The design goals of XML emphasize simplicity, generality, and usability over the Internet. It is a textual data format with strong support via Unicode for different human languages. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.

Many application programming interfaces (APIs) have been developed to aid software developers with processing XML data, and several schema systems exist to aid in the definition of XML-based languages. The material in this section is based on the XML Specification. This is not an exhaustive list of all the constructs that appear in XML; it provides an introduction to the key constructs most often encountered in day-to-day use.

a) (Unicode) character:

By definition, an XML document is a string of characters. Almost every legal Unicode character may appear in an XML document.

b) Processor and application:

The processor analyzes the markup and passes structured information to an application. The specification places requirements on what an XML processor must do and not do, but the application is outside its scope. The processor (as the specification calls it) is often referred to colloquially as an XML parser.

MD5 digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. The MD5 message The security of the MD5 hash function is severely compromised. A collision attack exists that can find collisions within seconds on a computer with a 2.6 GHz Pentium 4 processor (complexity of 224.1).[25] Further, there is also a chosen-prefix collision attack that can produce a collision for two inputs with specified prefixes within hours, using off-the-shelf computing hardware (complexity 239).[26] The ability to find collisions has been greatly aided by the use of off-the-shelf GPUs. On an NVIDIA GeForce 8400GS graphics processor, 16–18 million hashes per second can be computed. An NVIDIA GeForce 8800 Ultra can calculate more than 200 million hashes per second

Windows Communication Foundation (WCF) is a tool often used to implement and deploy a service-oriented architecture (SOA). It is designed using service-oriented architecture principles to support distributed computing where services have remote consumers. Clients can consume multiple services; services can be consumed by multiple clients. Services are loosely coupled to each other. Services typically have a WSDL interface (Web Services Description Language) that any WCF client can use to consume the service, regardless of which platform the service is hosted on. WCF implements many advanced Web services (WS) standards such as WS-Addressing, WS- Reliable Messaging and WS-Security. With the release of .NET Framework 4.0, WCF also provides RSS Syndication Services, WS-Discovery, routing and better support for REST services.

4. SYSTEM REQUIREMENT AND SPECIFICATION

4.1. SOFTWARE AND HARDWARE REQUIREMENT:

In this section we describe the environment in which the software will operate, including hardware platform, versions and any other software components or applications with which it must peacefully exist.

4.1.1. SOFTWARE REQUIREMENT:

Operating System:-Windows.

Language: - .NET, (WCF: - Windows Communication Foundation).

Front end: - .NET.

Documentation: - LATEX.

4.1.2. HARDWARE REQUIREMENT:

Processor: - PENTIUM III 866 MHS.

RAM: - 128 MD SD RAM.

MONITOR: - 15” Color.

HARD DISK: - 20 GB.

FLOPPY DRIVE: - 1.44 MB.

CD DRIVE: - LG 52X.

KEYBOARD: - STANDARD 102 KEY.

MOUSE: - 3 BUTTONS.

DEVICES: - Router, Server, Mobile.

4.1.3. USER REQUIREMENT:

User should register himself/herself with mobile no and valid Account number at server side.

1. User Login to the system through username.

2. Click points are used as a password.

3. While login, user A attached file to mail and send to user B.

4. Check some security technique by server side.

5. Check leading and trailing bits.

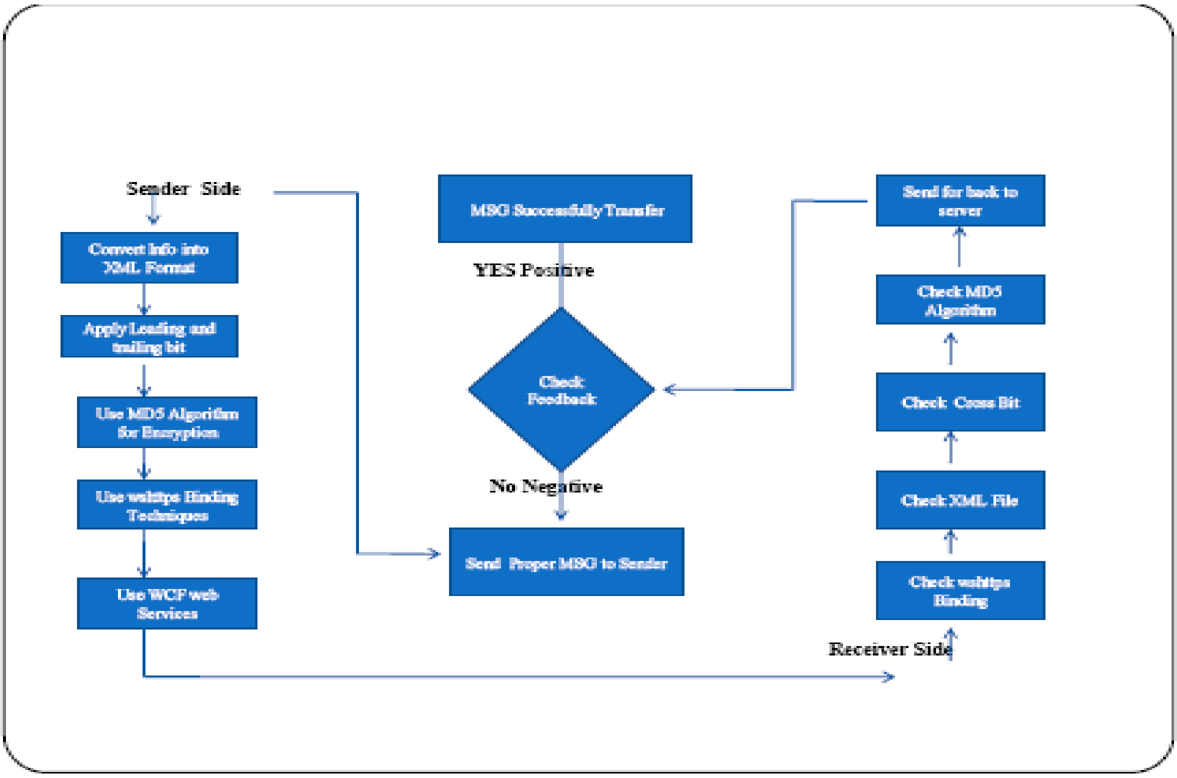
6. Generation of xml file.

7. Generation of hash value using Message Digest 5 Algorithm.

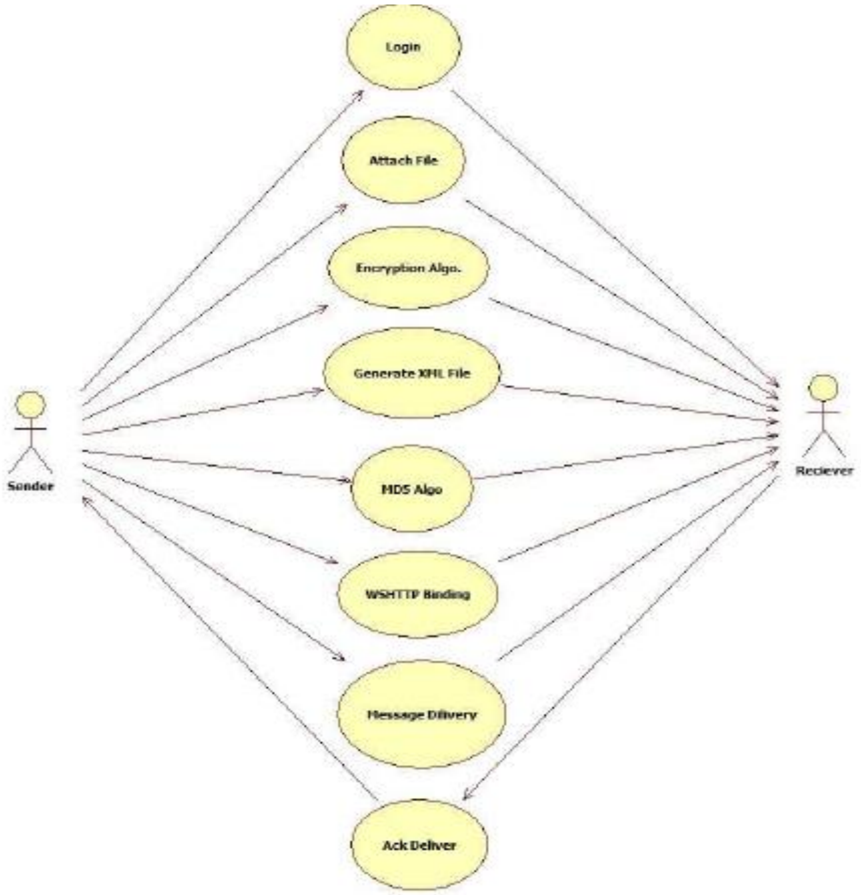
8. User B received file Successful.

4.2. GATHERING AND ANALYSIS USING UML:

4.2.1. WORKFLOW OF SYSTEM:

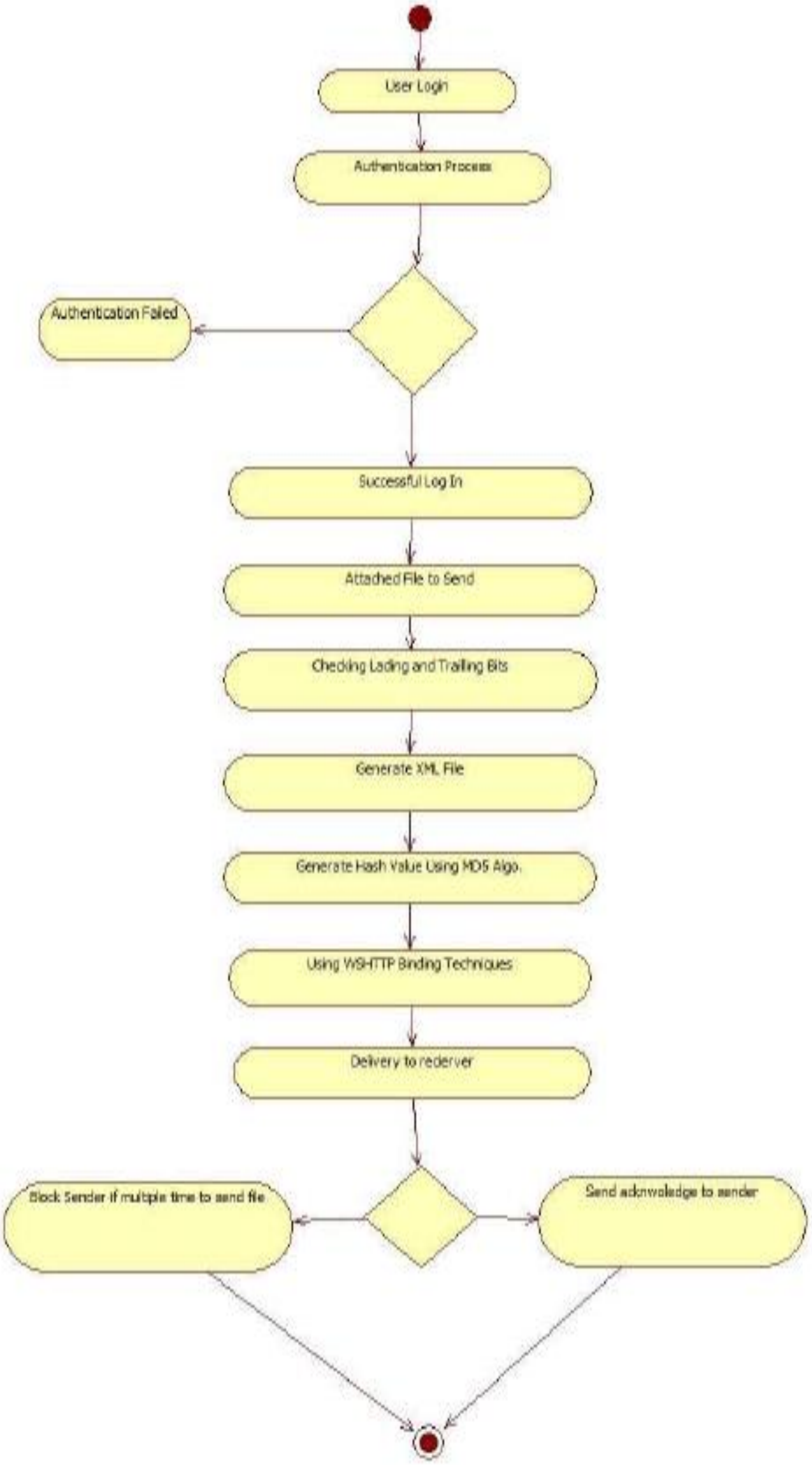


4.2.2. USE CASE DIAGRAME:

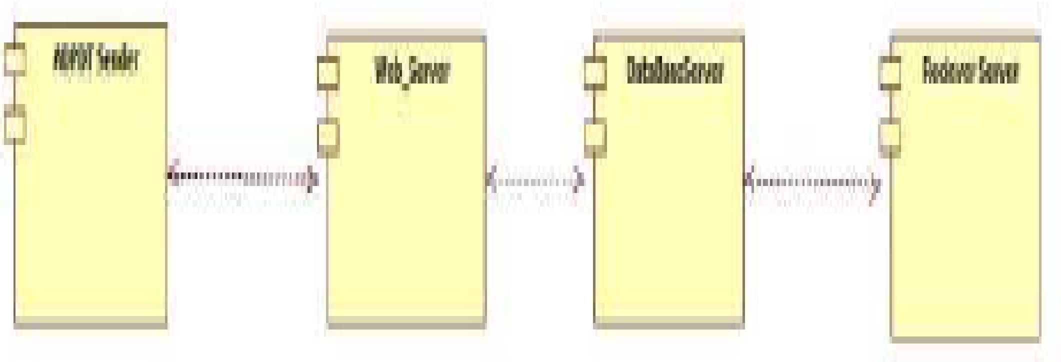


Use Case Diagram for System

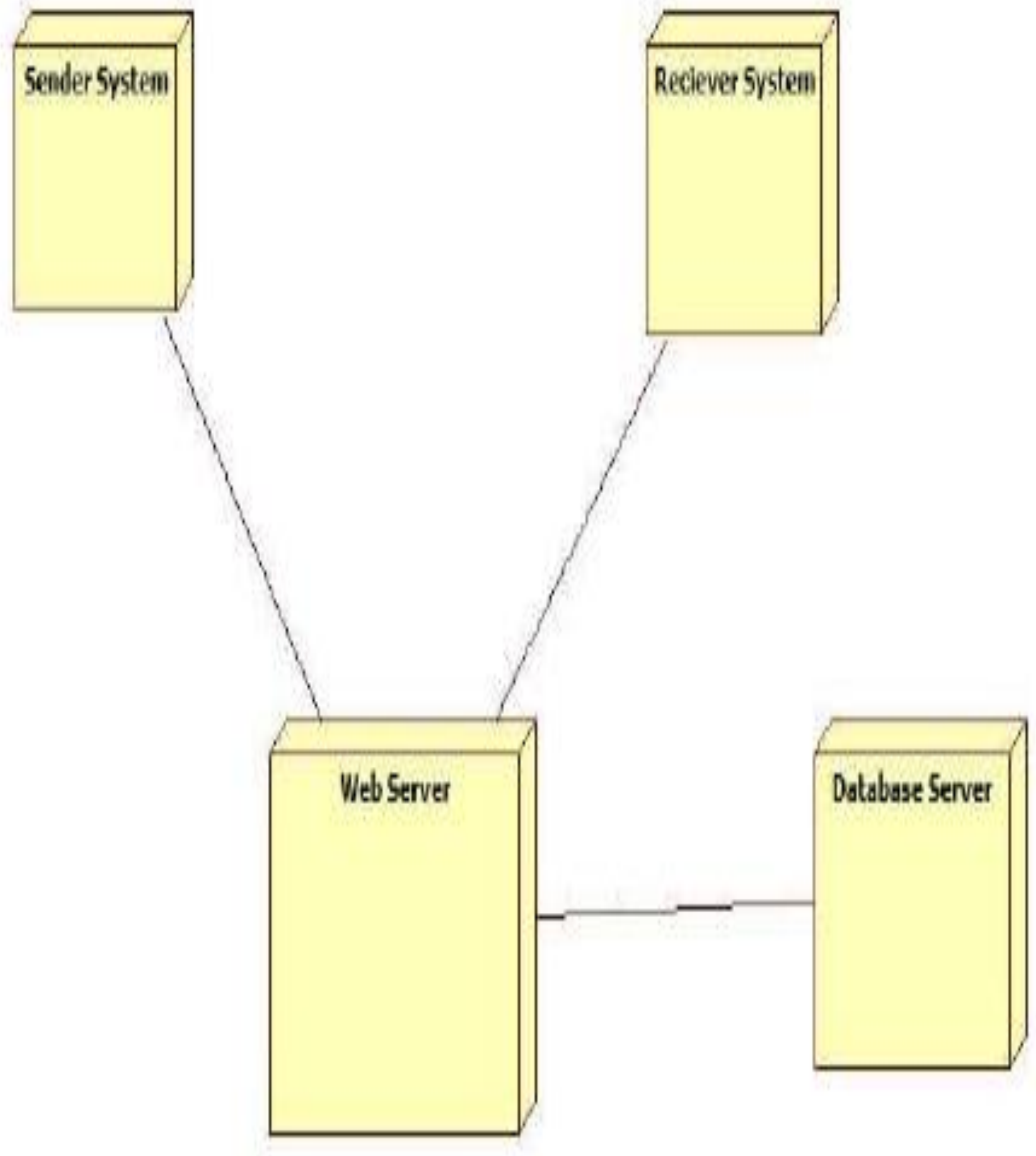
4.2.3. ACTIVITY DIAGRAM:


User Login
Authentication Process
Authentication Failed
Successful Log In
Attached File to Send
Checking Lading and Trailing Bits
Generate XML File
Generate Hash Value Using MD5 Algo.
Using WSHTTP Binding Techniques
Delivery to rederver
Block Sender if multiple time to send file
Send acknowledge to sender

4.3.2. COMPONENT DIAGRAM:

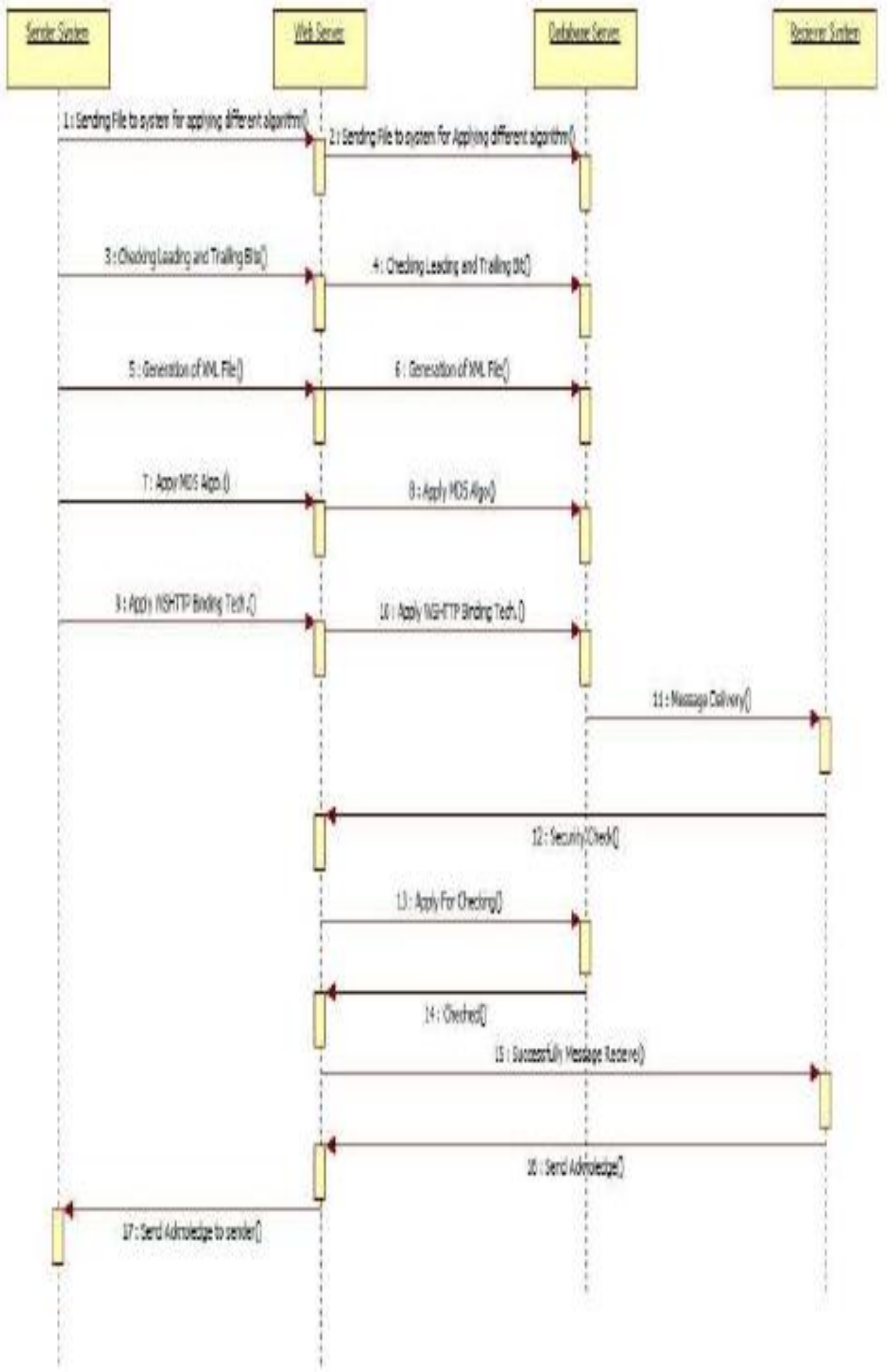


4.3.3. DEPLOYMENT DIAGRAM:

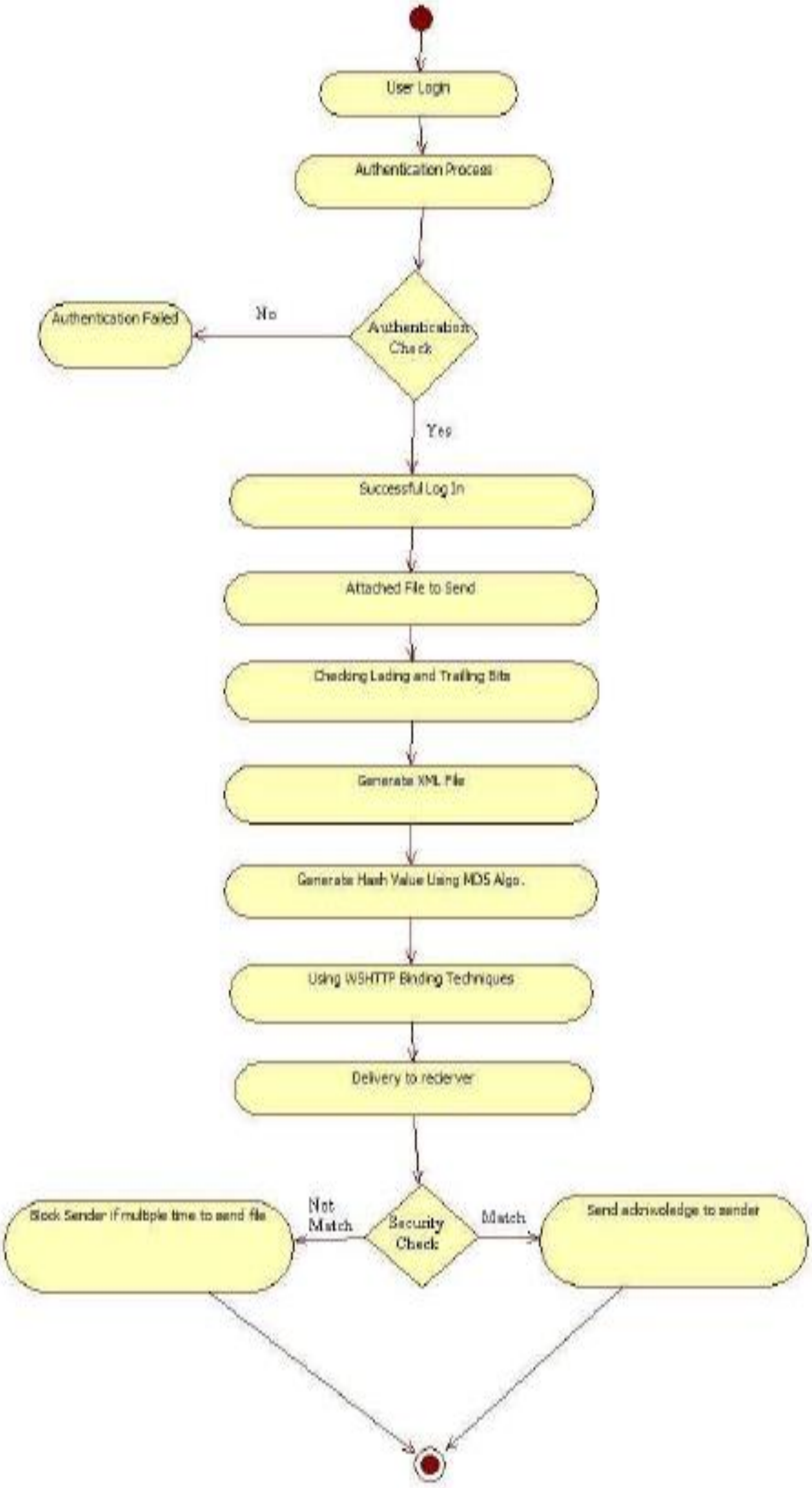


4.3. UML DIAGRAM:

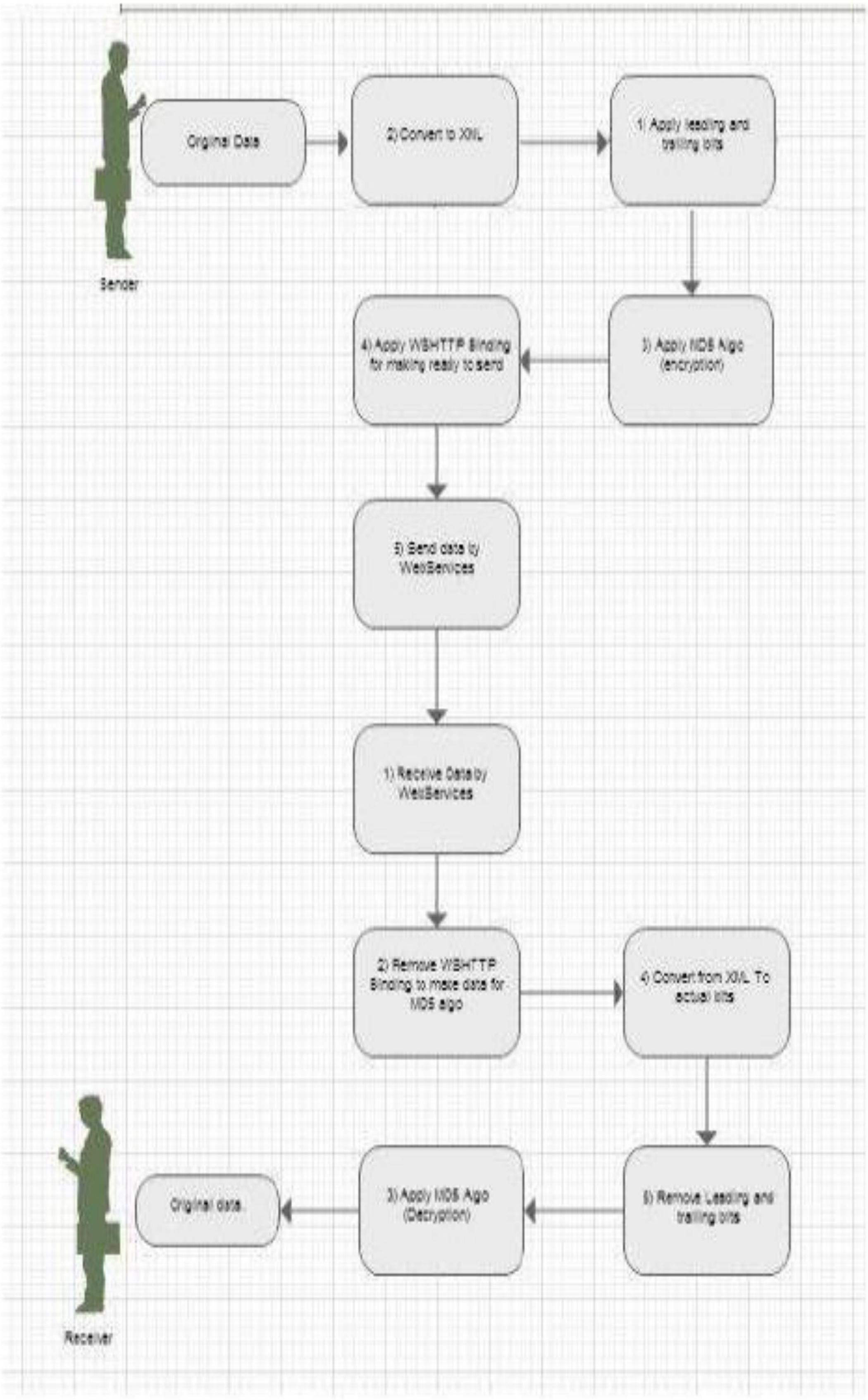
4.3.1. SEQUENCE DIAGRAM:


Sender System
Web Server
Database Server
Reciever System
1 : Sending File to system for applying different algorithm()
2 : Sending File to system for Applying different algorithm()
3 : Checking Leading and Trailing Bits()
4 : Checking Leading and Trailing Bit()
5 : Generation of XML File()
6 : Generation of XML File()
7 : Apply MD5 Algo ()
8 : Apply MD5 Algo()
9 : Apply WSHTTP Binding Tech.()
10 : Apply WSHTTP Binding Tech.()
11 : Message Delivery()
12 : Security Check()
13 : Apply For Checking()
14 : Checked()
15 : Successfully Message Recieve()
16 : Send Acknoledge()
17 : Send Acknoledge to sender()

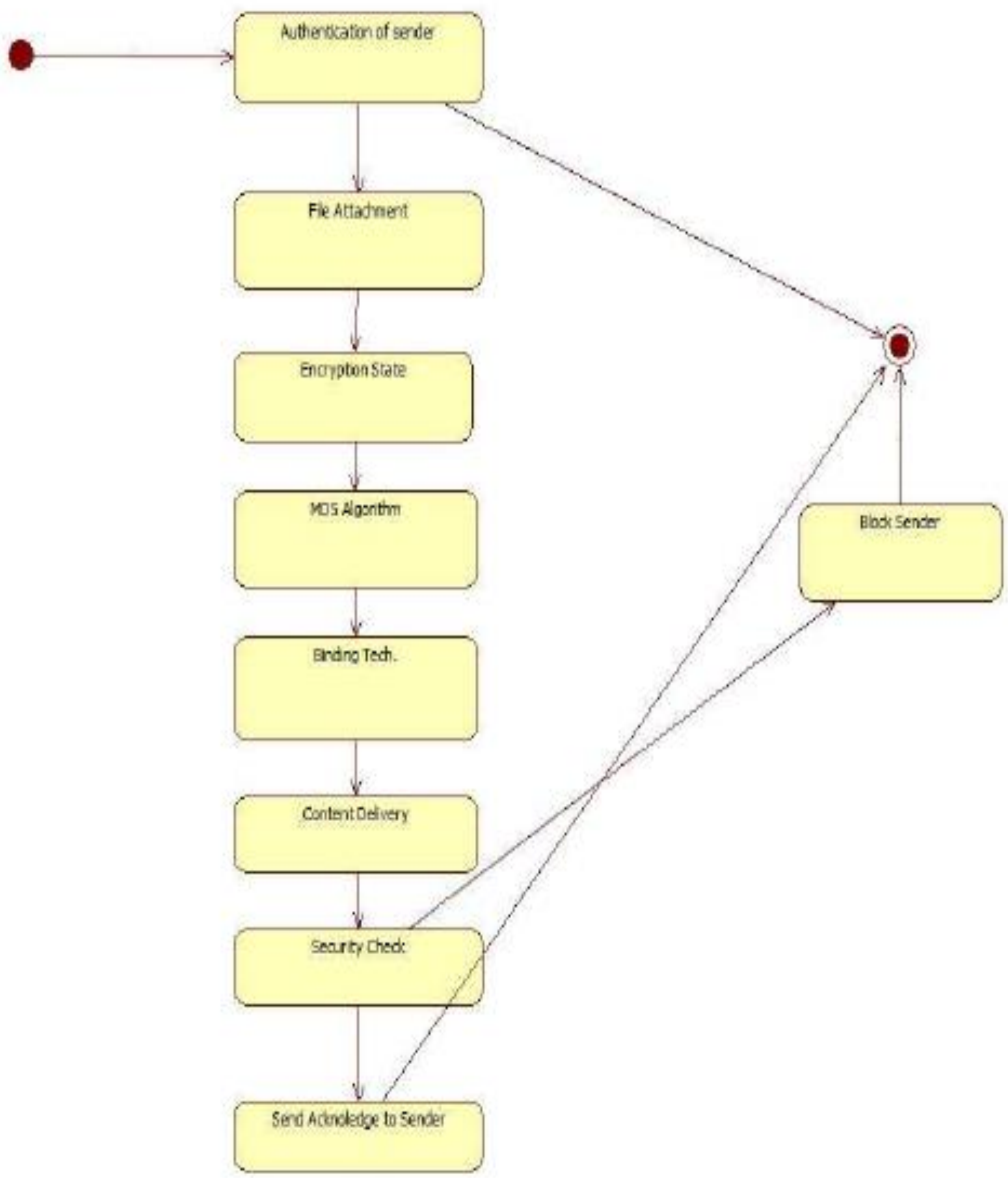
4.3.2. Activity Diagram:



4.3.3. Data Flow Diagram:


Sender
Original Data
2) Convert to XML
1) Apply leading and trailing bits
3) Apply MD5 Algo (encryption)
4) Apply WSHTTP Binding for making ready to send
5) Send data by WebServices
1) Receive Data by WebServices
2) Remove WSHTTP Binding to make data for MD5 algo
4) Convert from XML To actual bits
5) Remove Leading and trailing bits
3) Apply MD5 Algo (Decryption)
Original data
Receiver

4.3.4. State Chart Diagram:



5. PLANNING AND SCHEDULING

The objective of planning and scheduling is to introduce software project management and to describe its distinctive characteristics.

- To discuss the task of software project management and the project planning process.
- To show how graphical schedule representatives are used by project management.
- To discuss the notation of risks and the risk management process (same risks arise in software project).

ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. Pankaj P. Waghralkar and Head of the Department Prof. Sonali Madankar for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of PVPIT, Bavdhan for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1] Dantu K., Rahimi M.H. "Robomote: Enabling mobility in sensor networks" in 2005

[2] Bashir Yahya will appear in Wiley series, "Energy efficient MAC protocols in Wireless Sensor Networks" in 2009

[3] T Dam and K Langendoen, "An adaptive energy efficient MAC protocol for Wireless Sensor Networks" in 2003

[4] D Zeinalipour-Yazti, H. Papadakis, M. D. Dikaiakos, "Mobile sensor network Data Management" Parallel processing letter journal, sept. 2008.

[5] Lingxuan Hu and David, "Localization for Mobile sensor networks", International conference on mobile computing and networking, 2004.

[6] Allred J., Hasan A.B. Gray P, Mohseni K., "SensorFlock: An Airborne Wireless sensor network of Micro-air Vehicles", in 2007.

[7] Nittel S., Trigoni N., Nural A., "A drift-tolerant model for data management in ocean sensor networks", in 2007.