An efficient algorithm on secure data communication in the resource constrained network

Vijay Sai Chimata, Yashaditya Singh, Tenzin Topjor, Bharath B M
B.E. Students
Department of Computer Science and Engineering BMS College of Engineering Bangalore, India

Pradeep S, Assistant Professor Department of Computer Science and Engineering
BMS College of Engineering Bangalore, India

Abstract - Different sort of systems are dependable to share the information between sources to goal. Diverse kind of gadgets, for example, portable, workstation, sensors are taking an interest on the system correspondence. In light of the functionalities of system it is arranged as remote sensor organize, versatile adhoc arrange, vehicular adhoc system and IOT empowered system. Each sort of system utilized in various sort of utilizations. In any case each system is having the general example of information correspondence between the hubs which are taking part on the system. Delicate data's likewise transmitted over the system which requires abnormal state security. Security dangers is a noteworthy issue in the system correspondence. Gadget Cloning, Sensitive Data Exposure, Denial of Service, Unauthorized Device Access and Control, Tampering Data are the conceivable security dangers in the system. In this proposition a safe validation framework is talked about to maintain a strategic distance from gadget cloning and disavowal of administration assault.

Keywords – Security, Network, Encryption, Secret Key

I. INTRODUCTION

The system of vehicles, gadgets, boulevards, structures and different things inserted with the product, sensors, hardware and system availability. That empowers us the items to gather and trade data. These gadgets that trade data to cloud, where information is dissected and important administrations are offered can be undermined or broken by noxious clients for monetary benefit or cause notoriety harm to a focused on association or client. Most regular assaults are: Guidelines for Manuscript Preparation Cyber security is set of advances and procedures intended to shield frameworks in a system from outside and inner assaults, unapproved access or obliteration. A digital security framework comprises of two primary parts a system security framework and host security framework, both with at least firewalls, antivirus programming and Intrusion Detection System (IDS). IDS help distinguish unapproved use, modification, duplication, and annihilation of data systems1. There are three kinds of digital examination in help for IDS – Misuse based, Anomaly based, Hybrid based. Abuse locators identify assaults situated in known marks and require visit refreshes. They can't distinguish multi day or novel assaults however create least false rate. Oddity identifiers, model system and framework conduct and distinguish deviations from ordinary conduct. Skilled to identify novel assaults and can be utilized to characterize marks for abuse identifiers. This technique has conceivably high false caution rates. Half and half finders consolidate abuse and irregularity discovery and are utilized to expand the identification rates and lessening false positive rate of obscure assaults.

II. IMPLEMENTATION

This paper implements three main modules
1.Node creation
2.Key generation
3.Secure data transaction

1.Node Creation
Node creation consist of two parts.

User Device Initialization
In this module n number of user device will be created with the capacity to transfer the data to server node.A unique Mac id is assigned to each of the device to navigate through the network.

Server Node Initialization
In this module 'n' server system will be created with unlimited energy resource.Server is responsible to collect the data from user devices.Just like a User device creation, a unique Mac id is assigned to each of the server created.As per proposal session key based encrypted data transaction will be followed by server as communication pattern.

2.Key Generation
Since data is being encrypted and decrypted before and after the transaction, a unique Key which is only known to the sender and receiver is generated to encrypt and decrypt.Network is created between the two ends in following process.

Join Request
In this module the node which is going to send the data will request for communication bond with server node with the help of its secret key. For each device unique mac ID will be assigned to validate the integrity of the node.

Session request
Once join request is accepted by server node, user will request for session key for data transaction. Server node will encrypt the session key with the help of secret key of requester and it will forward

to requester node.

3.Data transaction
In this module data will be encrypted using session key and AES encryption algorithm and will be forwarded to server node. Server will decrypt the data by using session key. Invalid key results in failure of decryption process.

Functional Requirements
In order to transmit data safely and securely over the network, the data needs to be encrypt in such a way that it cannot be accessed while transmitting through the network.Hence AES encryption algorithm is used in order to securely transmit the data.

OPERATION OF AES
AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs and others involve shuffling bits around.
Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

NON FUNCTIONAL REQUIREMENTS

The performance requirement is usually measured in terms of response time for a given screen transaction per user. In addition to response time, performance can also be measured in transaction throughput, which is the number of transactions in a given time period, usually one second. For example, you could have a performance measurement that could be no more than three seconds for each screen form or a transaction throughput of one hundred transactions in one second. Regardless 9 of the measurement, you need to create an architecture that allows the designers and developers to complete the system without considering the performance measurement.

Reliability ensures the integrity and consistency of the application and all its transactions. As the load increases on your system, your system must continue to process requests and handle transactions as accurately as it did before the load increased. Reliability can have a negative impact on scalability. If the system cannot maintain the reliability as the load increases, then the system is really not scalable. So, for a system to truly scale it must be reliable.
Extensibility is the ability to add additional functionality or modify existing functionality without impacting existing system functionality. You cannot measure extensibility when the system

is deployed, but it shows up the first time you must extend the functionality of the system. You should consider the following when you create the architecture and design to help ensure extensibility: low coupling, interfaces, and encapsulation.

Security is the ability to ensure that the system cannot be compromised. Security is by far the most difficult systemic quality to address. Security includes not only issues of confidentiality and integrity, but also relates to Denial-of-Service (DoS) attacks that impact availability. Creating an architecture that is separated into functional components makes it easier to secure the system because you can build security zones around the components. If a component is compromised, then it is easier to contain the security violation to that component.

DATA FLOW MODEL

Data Flow model is a way of representing how a data is processed inside the particular system.It also shows how a system executes in step by step.Notations used in the data flow model symbolise information motions, storage of information and cognitive planning between tasks. During the series of measures, these designs portray how information flows.

Data transformation takes place at each level before proceeding to the next level. These phases of conversion or handling are features of the program whereas representations of information stream are used to document a system layout. Any customer can comprehend how the scheme works, accomplishes and implements using the information stream template. It is possible to compare ancient data flow models with fresh data flow models attracted to develop more effective scheme.

Models of information flow are used to assist the end customer comprehend the entire scheme and how and where their information is used. Different modeling rules are kept in mind when developing the following DFDs:

Each process should contain one data for flow in and flow out.

- Each method should convert incoming information and generate fresh forms of outgoing information.
- ● Every data which is stored must involve in one data flow at least.
- ● External entity should be concerned with one data flow at least

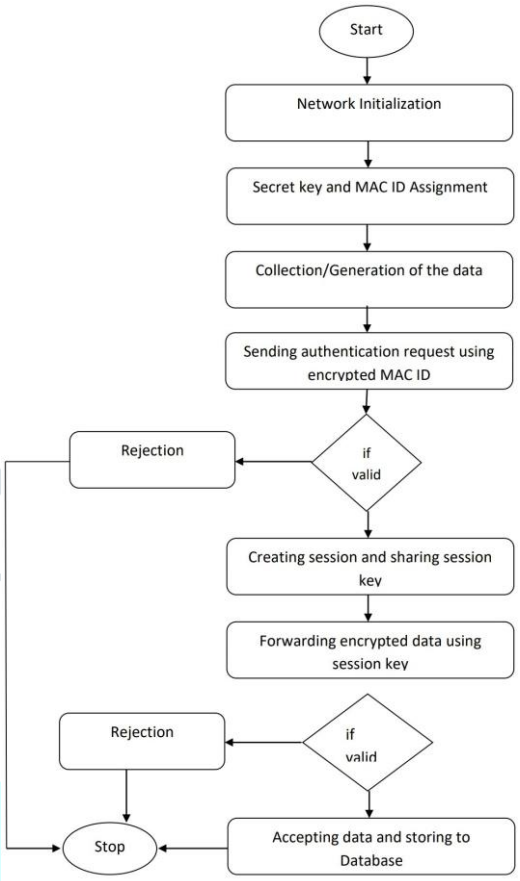

Figure 4.5 Flow Chart

Java

Java is object oriented programming language developed by sun micro system in 1992 later oracle corporation is acquired.

- Java is developed By James gosling and Patrick Naughton.
- Java is simple and easy programming language because complex features like operator overloading, multiple inheritance, pointers, and explicit memory allocation.

DBMS

Database management system is nothing but a collection of data stored and retrieve from this memory area is also called as database management system here two main things are required to optimize.

- **Storage of data**
- **retrieval of data**

JavaFX

JavaFX is a Java library that is used to develop Desktop applications as well as Rich Internet Applications (RIA). The applications built in JavaFX, can run on multiple platforms including Web, Mobile and Desktops.

JavaFX is intended to replace swing in Java applications as a GUI framework. However, It provides more functionalities than swing. Like Swing, JavaFX also provides its own components and doesn't depend upon the operating system. It is lightweight and hardware accelerated. It supports various operating systems including Windows, Linux and Mac OS.

Evaluation Metric

1. Energy consumption
   - ➢ This metric is calculated by using size of packet and consumption per bit.
2. Packet Delivery ratio
   - ➢ This metric is calculated by using ratio between received data and sent data.
3. Packet drop
   - ➢ This metric is identified as difference between sent packets and received packets.

EXPERIMENTAL RESULT

This model is coded in JAVA and is made run in NETBEANS. First we have created nodes and requested a session with the server. A secret key has been generated which can only be accessed by authorized users. An authorized user would be able to access the data using this unique secret key. Third party user like hackers could not access the data. The objectives have been successfully achieved.

III. CONCLUSION

The two security challenges that constitute max security breaches in electronic devices landscape have now solutions identified to prevent attacks. The unique solution implemented is carefully chosen due to hardware constraints of processing and memory on electronic devices as well as minimize cost of data transfer charged by ISP. Implementation is carried out to establish device connection with cloud component for authenticating devices to prevent device clone attacks.
Post successful authentication data is encrypted to prevent sensitive data exposure. The solution is efficient as it is very secure with very little overheads in terms of time required for authentication which is not exponential and data size which just adds additional 8 bytes of encrypted session key for every data posted from device to cloud. The little cost overhead is worth the huge security benefits.

IV. REFERENCES

1. Hyun-Jin Kim, Hyun-Soo Chang, Jeong-Jun Suh, A Study on Device Security in IoT Convergence, 2016 IEEE.
2. Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, Mark Vinkovits Denial- of-Service detection in 6LoWPAN based Internet of Things, 2013 IEEE.
3. Shaza Zeitouni,Yossef Oren,Christian Wachsmann, Remanence Decay SideChannel: The PUF Case, 2016 IEEE.
4. Debdeep Mukhopadhyay, PUFs as Promising Tools for Security in Internet of Things, 2015 IEEE.
5. Akashdeep Bharadwaj, Dr. G V B Subramanyam, Dr.Vinay Aasthi,Dr.Hanumat Sastry,Solutions for DDos attacks on cloud, 2016 IEEE.
6. Detect DoS attack using MrDR method in merging two MANETs, Albandari Alsumayt, John Haggerty , Ahmad Lot, IEEE 2016.