



World University of Bangladesh Computer Science and Engineering (CSE)

Welcome To Presentation On Design and Implementation of a Lightweight Encryption Algorithm for IoT Devices

Presented By...

Name : Arif Hussain
Roll : 1463
Batch : 33D

Name : Harun Ur Rashid
Roll : 1453
Batch : 33D

Name : Md. Riaz Rahman
Roll : 1458
Batch : 33D

Supervised By...

Md. Ashraf Kamal
Sr. Lecturer in Computer Science & Engineering
World University Of Bangladesh

Introduction

- ❑ Data Security is an important issue now a days. It is a digital privacy which is prevent unauthorized access to computer, database and websites.
- ❑ Billions of IoT devices that have sensing or actuation capabilities and are connected to each other via the Internet.
- ❑ Security has not been a high priority for these devices until enough now. It is now time to establish The Internet of Secure Things.
- ❑ By this project we want to develop an encryption algorithm for IoT devices.

IOT devices

Example :

- ❑ Smart watches
- ❑ Smart Glasses
- ❑ Smart fabrics
- ❑ E-textiles etc



Objectives

- ❑ To reduce processing complexity and provide powerful data security for wearable devices.
- ❑ To develop a lightweight encryption algorithm with small size of keys.

Methodology



Figure: Methodology

Our proposed model

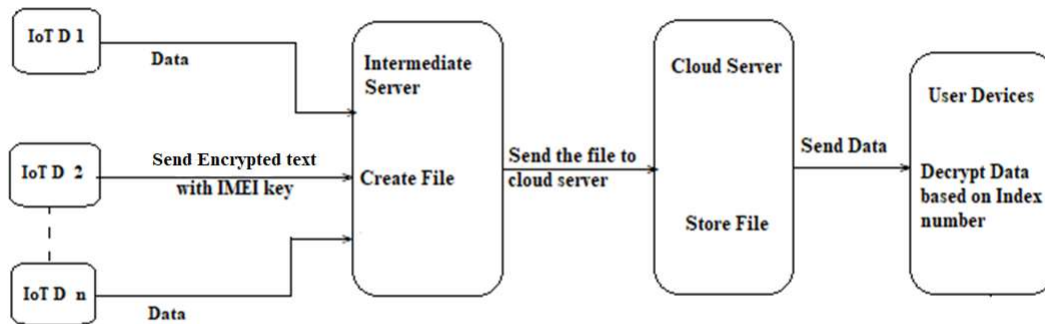


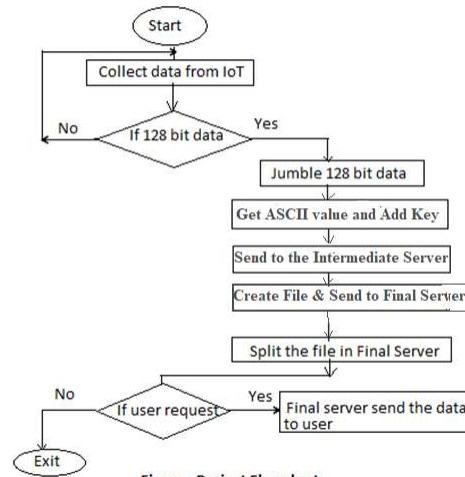
Figure: Proposed Model Block Diagram

Our proposed model Algorithm

The algorithm has the following features...

- Step-1: Collect 128 bit data from IoT devices.
- Step-2: Jumble 128 bit data and get key (index number).
- Step-3: Get ASCII value of the jumble data.
- Step-4: Add the ASCII value and key.
- Step-5: Send the encrypted data to the Intermediate Server.
- Step-3: Create a File of the encrypted data in Intermediate Server.
- Step-4: Send the File to Final Server.
- Step-5: Again, Final Server split the file into small file and send to the receivers.

Project Flowchart



Key Generate

Index number	0	1	2	3	4	5	6	7	8	9	10	11
Data	H	o	w		a	r	e		y	o	u	?

Index number	0	1	2	3	4	5	6	7	8	9	10	11
Jumble Data	e	?	y	o	r		o	H	u	w		a

Key	0	1	2	3	4	5	6	7	8	9	10	11
	7	6	9	10	11	4	0	5	2	3	8	1

How to Get Chipper Text/ Encrypted Data

Index number	0	1	2	3	4	5	6	7	8	9	10	11
Jumble Data	e	?	y	o	r		o	H	u	w		a

Index number	0	1	2	3	4	5	6	7	8	9	10	11
ASCII value	101	63	121	111	114	32	111	72	117	119	32	97

Index number	0	1	2	3	4	5	6	7	8	9	10	11
ASCII value + Key	101+7 =108	63+6 =69	130	121	125	36	111	77	119	122	40	98

Index number	0	1	2	3	4	5	6	7	8	9	10	11
Character Value	1	E	g	y	}	\$	o	M	w	z	(b

Original Text/Plain Text

Chipper Text/Encrypted Text

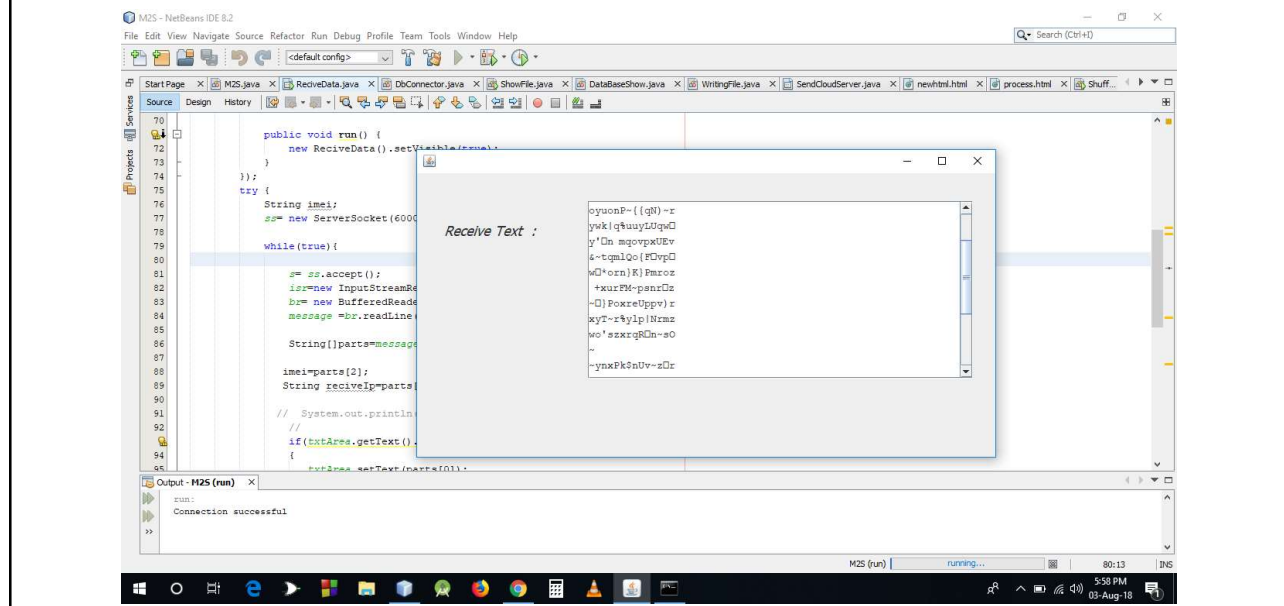
How are you?

1Egy}\$oMwz(b

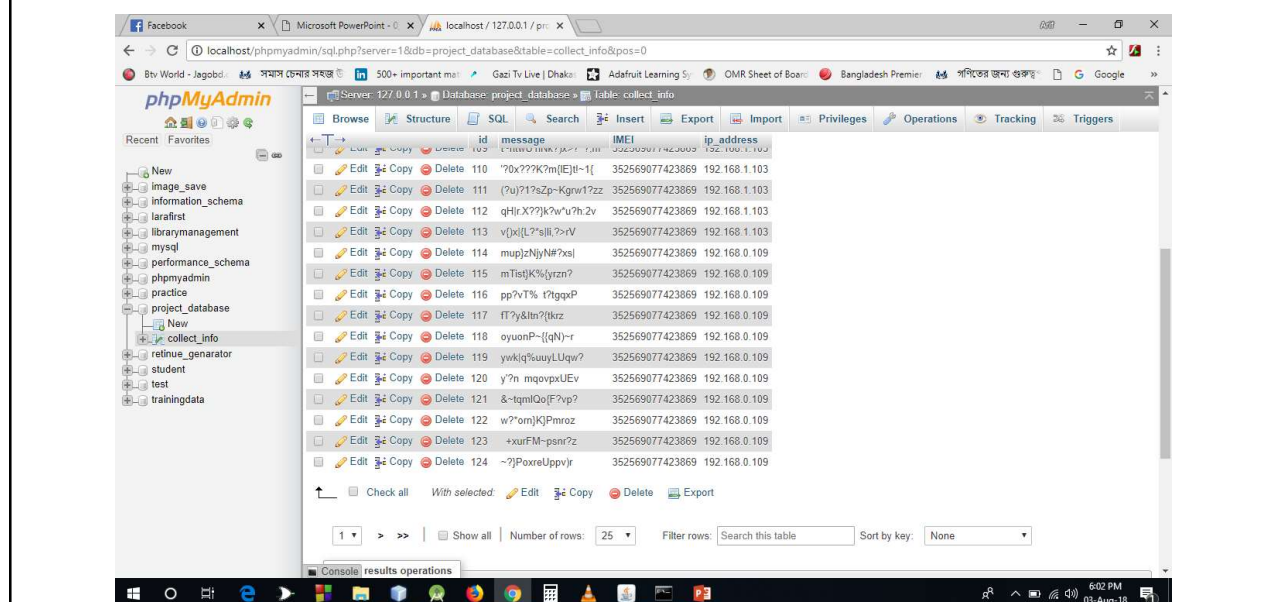
Design, Development and Testing (Get Encrypted Data and Send To the Intermediate Server)

The screenshot shows the M2Server application interface. It includes a blue header with the title "M2Server". Below the header, there are four input fields: "Enter IP Address" (containing "192.168.1.105"), "Enter Text" (containing "Hello, Everyone."), "Security Key" (containing "12611111479526158141613"), and a "SEND" button. At the bottom, there is an "Information" section with a list of instructions: (i) You must be connected same router network, (ii) Then you enter your ip address and text, (iii) Then click the send button, (iv) You must be open your pc socket program, (v) This app work only same network, same port address. The app is created by @AriF, @Harun, @Riaz and supervised by @Al-Amin Nipu, @Asraf Kamal (WUB).

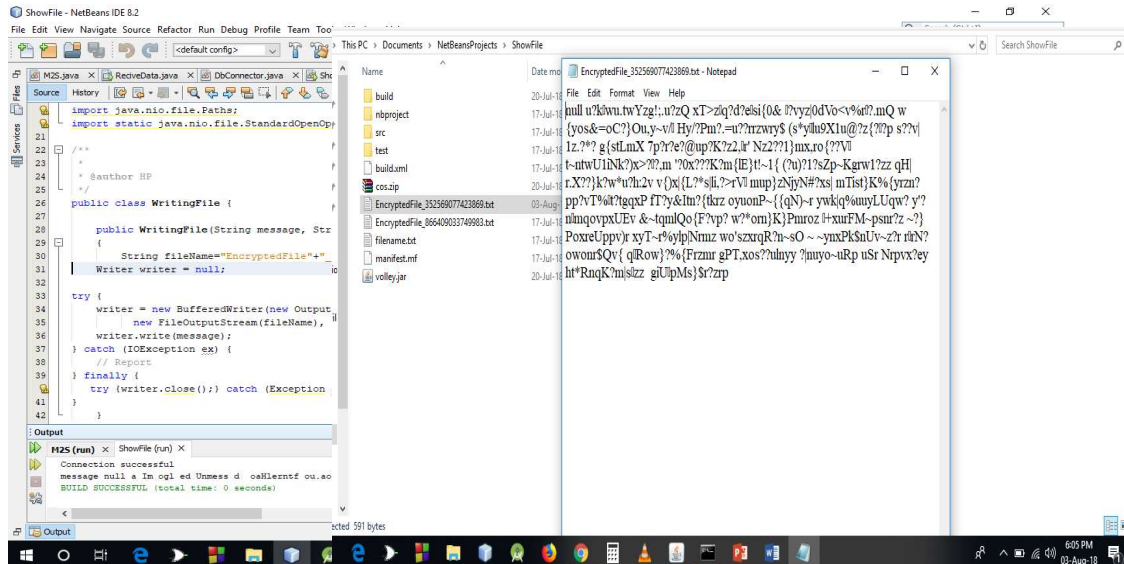
Development and Testing (Receiving Text by Intermediate Server)



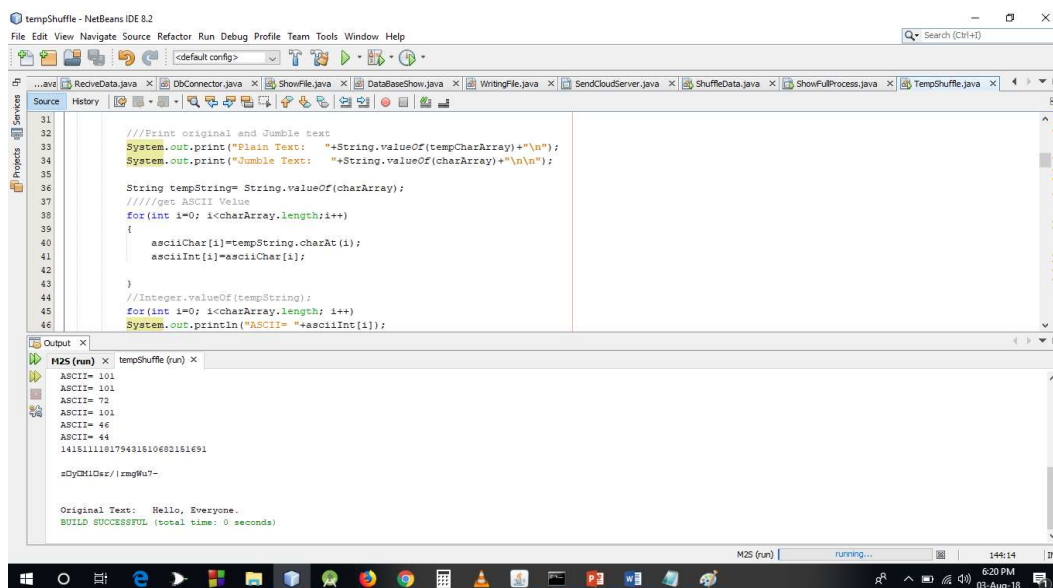
Development and Testing (Store the data by Intermediate Server)



Development and Testing (Create File by Intermediate Server)



Development and Testing (Decrypt Process)



Conclusion

- We understood that IoT based devices faces that number of challenges like power, bandwidth, scalability, heterogeneity, security and privacy.
- Now Security and Privacy is the most imperative challenge to solve to maintain the trust of users in IoT.
- So if we develop an encryption algorithm, we hope it will be so helpful for IoT based devices security. Though it is a small contribution.

Thank You All