Improvement and Survey of Fog Computing Using Encryption

S. Jansi Rani[1], Dr. Selvakani[2], Mrs. K. Vasumathi[3]

[1]PG Scholar, PG Department of Computer Science,
Government Arts and Science College, Arakkonam, Ranipet, Tamilnadu, India,
Jansirani26112001@gmail.com
[2]Assistant Professor and Head,
PG Department of Computer Science, Government Arts and Science College,
Arakkonam, Ranipet, Tamilnadu, India,
sselvakani@hotmail.com
[3]Assistant Professor and Head,
PG Department of Computer Applications, Government Arts and Science College,
Arakkonam, Ranipet, Tamilnadu, India,
kulirmail@gmail.com

Abstract

This research develops a fog computing-based encrypted manipulate machine in a practical industrial placing. The evolved system conceals controller profits and signals over communique links the usage of multiplicative holomorphic encryption to prevent eavesdropping assaults. Experimental validation confirms the feasibility of function servo manipulate for the motor driven degree with the developed machine in phrases of overall performance degradation, parameter version, and processing time. The evolved machine inherits its stability no matter whether plant parameters range or no longer even after the controller profits and indicators are encrypted. Furthermore, despite the fact that processing time becomes longer by way of increasing a key length of encryption, degradation of control performance is advanced simultaneously.

Keywords: Networked robots, robot safety, motion control, encryption control, fog computing.

1. INTRODUCTION

Cloud based manage structures, in which controlled gadgets are connected to a conversation community to be monitored and controlled with in cloud, are gaining recognition. control as a service (CAAS)for car control, A cloud primarily based control concept was proposed in.

Fog computing gives many capability blessings, In particular for actual time programs, even though safety and privateness issues in the fog persist just like the case of the cloud. Attacks on cyber physical system, along with networked manage systems, are greater unfavourable than attacks on records structures due to the fact physical systems can at once have an effect on actual environments.

Encrypted control, a fusion of cryptography and manipulate theory, is a promising method to enhance the security of control structures by means of reducing risks of eavesdropping attacks. In encrypted control systems the use of encryption, which is multiplicative homomorphic encryption, control inputs are calculated in cipher text from encrypted controller parameters, encrypted sensor records, and an encrypted reference without decryption.

2. LITERATURE SURVEY

TITLE: CLOUD CONTROL SYSTEMS
AUTHOR: Y. Xia
YEAR: 2015
DESCRIPTION:

The concept of cloud control systems is discussed in this paper, which is an extension of networked control systems (NCSs). With the development of internet of things (IOT), the technology of NCSs has played a key role in IOT. At the same time, cloud computing is developed rapidly, which provides a perfect platform for big data processing, controller design and performance assessment. The research on cloud control systems will give new contribution to the control theory and applications in the near future.

TITLE: SECURE REAL-TIME CONTROL THROUGH FOG COMPUTATION
AUTHOR: K. Sato and S. Azuma
YEAR: 2019
DESCRIPTION:

Consider an asymptotic stabilization problem with a specified confidential level for an Internet of Things system composed of the Cloud, Fog, and a controlled device. A sequence of concealed states, that is, a sequence of the sum of the true state of a controlled device and artificial noise, termed the security input, is transferred to the Fog. As the method for concealing the true state is relatively simple, it enables us to achieve rapid real-time communication between a controlled device and the Fog. The level of confidentiality was measured using the mutual information between the true and concealed states. As a solution to our problem, we obtained Gaussian-type security inputs and a convex optimization problem for calculating feedback gains. Moreover, we proved that the main solution becomes

all solutions for any scalar cases. Finally, we demonstrated the feasibility of our proposed method by solving the problem of tracking the reference signal of storage batteries in smart grids.

TITLE: SECURITY AND TRUST ISSUES IN FOG COMPUTING: A SURVEY
AUTHOR: P. Zhang, M. Zhou, and G. Fortino
YEAR: 2018
DESCRIPTION:

Fog computing uses one or more collaborative end users or near-user edge devices to perform storage, communication, control, configuration, measurement and management functions. It can well solve latency and bandwidth limitation problems encountered by using cloud computing. First, this work discusses and analyzes the architectures of Fog computing, and indicates the related potential security and trust issues. Then, how such issues have been tackled in the existing literature is comprehensively reported. Finally, the open challenges, research trends and future topics of security and trust in Fog computing are discussed.

TITLE: FOG COMPUTING FOR THE INTERNET OF THINGS: SECURITY AND PRIVACY ISSUES
AUTHOR: A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng
YEAR: 2017
DESCRIPTION:

The inherent characteristics of Internet of Things (IoT) devices, such as limited storage and computational power, require a new platform to efficiently process data. The concept of fog computing has been introduced as a technology to bridge the gap between remote data centers and IoT devices. Fog computing enables a wide range
of benefits, including enhanced security, decreased bandwidth, and reduced latency. These benefits make the fog an appropriate paradigm for many IoT services in various applications such as connected vehicles and smart grids. Nevertheless, fog devices (located at the edge of the Internet) obviously face many security and privacy threats, much the same as those faced by traditional data centers. In this article, the authors discuss the security and privacy issues in IoT environments and propose a mechanism that employs fog to improve the distribution of certificate revocation information among IoT devices for security enhancement. They also present potential research directions aimed at using fog computing to enhance the security and privacy issues in IoT environments.

TITLE: **FUNDAMENTAL ISSUES IN NETWORKED CONTROL SYSTEMS**
AUTHOR: M. S. Mahmoud and M. M. Hamdan
YEAR: 2018
DESCRIPTION:

This paper provides a survey on modeling and theories of networked control systems (NCS). In the first part, modeling of the different types of imperfections that affect NCS is discussed. These imperfections are quantization errors, packet dropouts, variable sampling/transmission intervals, variable transmission delays, and communication

constraints. Then follows in the second part a presentation of several theories that have been applied for controlling networked systems. These theories include: input delay system approach, Markovian system approach, switched system approach, stochastic system approach, impulsive system approach, and predictive control approach. In the last part, some advanced issues in NCS including decentralized and distributed NCS, cloud control system, and co-design of NCS are reviewed.

3. MODULES

- USER
- FOG SERVER
- CLOUD SERVER

A. Module Description

1. USER

User is the owner of data. Privacy, disaster recoverability, modification detection of user's data is ultimate goal of this paper.

2. **FOG SERVER:**

Fog server is trusted to user. User relies on fog server with his data. Close proximity of fog devices to the user, robust physical security, proper Authentication, secure communication, intrusion detection ensures fog server's reliability to the user.

3. CLOUD SERVER:

Cloud server is considered as honest but curious. This means that cloud server follows the Service Level Agreement (SLA) properly, but has an intention to analyze user's data. Conversely, cloud server may pretend to be good but acts as a potential adversary. In that case, cloud server may modify data in order to forge as original data. Similarly, cloud server may hide/loss the data resulting in permanent data loss of the user. Furthermore, hardware/software failure may result in data modification or permanent loss as well.

4. DEVELOPED SYSTEM

This area introduces the structure of the cloud and fog computing-based control machine as well as its specifications. Furthermore, a C language library for the encrypted manage is described.

A. Concept

Illustrates a thought concept of the fog computing-based control system with a Public cloud. Company A administrates a cloud infrastructure and presents a platform to operate the higher-layer control. Company B, C, and D control fog connected to the cloud and every other. Company B and C may also be branches of Company D, and they aim to manage devices, which include some actuators and are owned by each company. An operator sends duties for the higher-layer manipulate to an application in the cloud. The utility generates reference indicators to implement the tasks and transfers them to the fog. The fog decides the enter alerts from the reference alerts and sensor data of the devices in actual time. Additionally, the fog handles operating data and transfers them to the cloud. The cloud storages the data and visualizes them with a web interface for the operator.

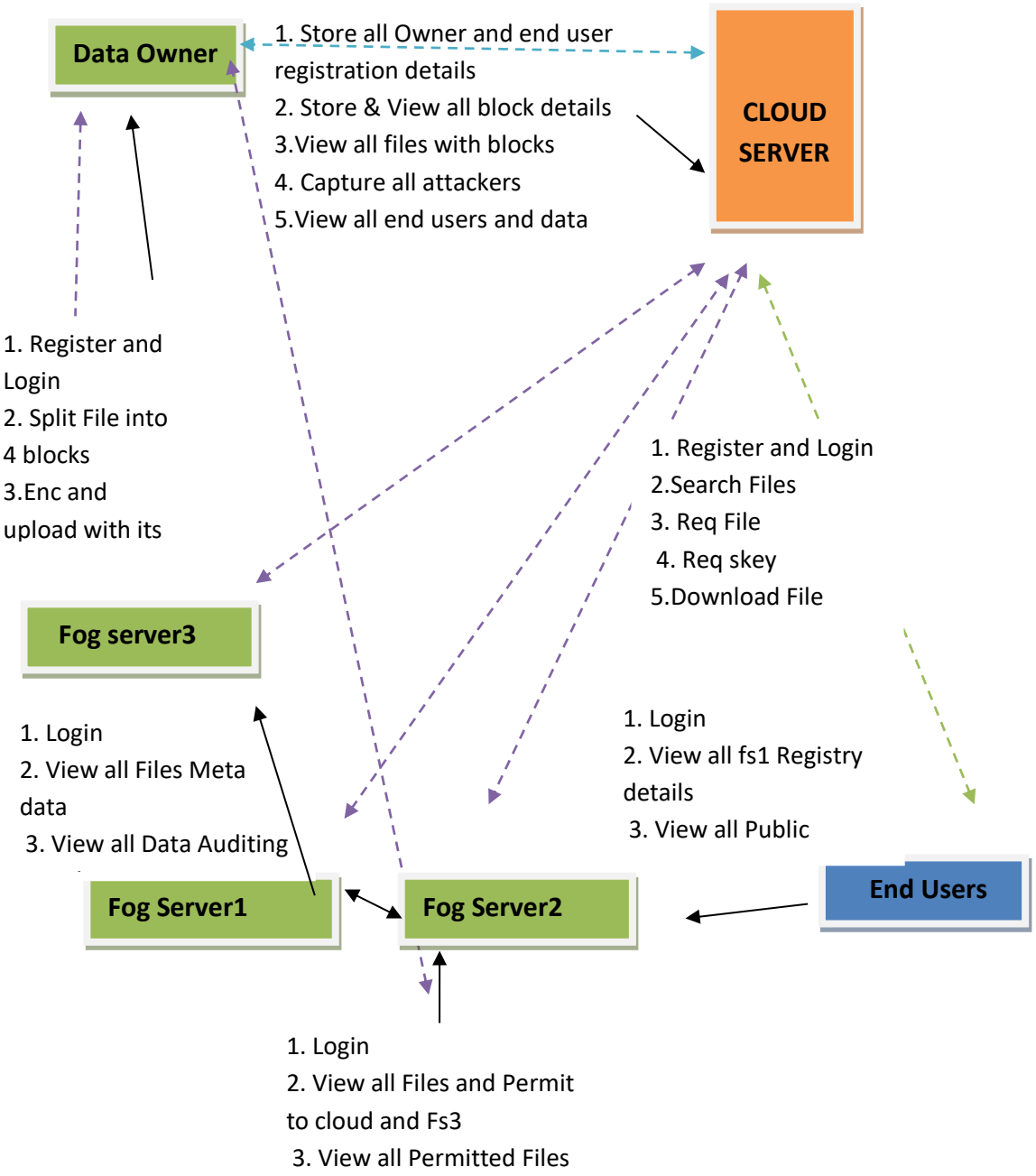
B. Specification

The developed system consists of a motor-driven stage, the plant-side computer, and the fog-side computer. Their specifications are described in Table I. Motor-driven ranges or linear actuators are predominant factors for factory automation. The stage is moved by way an AC servo motor through a slide screw, as proven, and the AC motor and the slide scre ware connected by means of a coupling. The AC motor with the attached rotary encoder is pushed by means of the servo amplifier, and we use the servo amplifier as a modern controller as it has adequate manipulate bandwidth. Note that though the developed gadget uses a slide screw, the protection enhancement technique Section II can additionally be applied to a machine that uses a ball screw or other linear
Actuators.

C. Architecture

This letter focuses on growing the fog computing-based control machine within the blue body seen in illustrates the network structure of the developed system. We use non-public computers for a fog-computing environment and the interface between a managed device and the network. The computers are linked to L2 switches, which in turn are connected to an L3 switch through an Ethernet cable. Additionally, as per the necessities of a logical network, each computer system are installed in the identical VLAN. The computers speak with every different via other via TCP/IP socket communication, and the L3 switch addresses routing decisions.

4. SYSTEM ARCHITECTURE



5. EXPERIMENTAL RESULTS

This area offers the outcomes of some experiments for validating the developed system. Effect of load fluctuation and real-time computation in the proposed system are also indicated.

A. PERFORMANCE DEGRADATION AND SYSTEM CONCEALMENT

It is nicely recognised that the addition of a quantizer in a manage loop decreases the overall performance of the manage system. Thus, the control performance of the encrypted PID manage system is anticipated to be worse than that of a ordinary PID manipulate machine because Q acts as a quantizer. This find out about consists of investigation of the control overall performance deterioration prompted by means of encryption in order to verify the practicality of the proposed system. The validations of the obtain and sign concealment are additionally blanketed.

B. EFFECT OF LOAD FLUCTUATION

Industrial robots procedure more than a few duties by changing their give up effector according to the work content. Their mannequin parameters depend on their posture and hand mass. This parameter fluctuation influences the overall performance of the tracking control and steadiness of the control systems. Therefore, in order to practice the controller encryption technique to the control systems, it is vital for the encrypted manage device to hold steadiness underneath uncertain conditions. This find out about examines the behavior of the developed device with a 10 kg load on the stage, as proven in Fig. 3(b), by way of conducting the identical experiment as Section IV-A. This load fluctuation impacts the second of inertia and the viscous friction of the stage, leading to a change in the time constant. Fig. 7 indicates the effects of the monitoring manipulate with the load. These effects are similar to those in Fig. 5, which capacity that the overall performance of the encrypted controller is impartial of uncertainty due to load fluctuations. In different words, the steadiness of the encrypted manipulate machine with enough length key is decided only by means of the original controller properties.

C. PROCESSING TIME

A key of longer length makes the ciphertext stronger. On the different hand, the encrypted controller increases processing time as the key size increases. Hence, the key size cannot be extended indiscriminately due to the fact real time computation is vital for industrial manage systems. This study measures the time taken to execute the encrypted manage in the developed system with the library, and describes the relationship between the key size and processing time. The key length is changed from 32 bits to 1024 bits, and the processing time, excluding the communication time, is measured 100,000 times for each key length. Then, the most processing time, minimum processing time, and suggest processing time are obtained. Table III and Table IV list the effects of the processing time, and visualizes these results. The times for the plant side . Extend exponentially with the key length. In contrast, the instances of fog facet are nearly proportional to it. These consequences point out that they enlarge in processing time required for Enc and Dec+ is massive in contrast to Mult.

Note that the consequences can't be compared with the processing time of other methods due to the fact the proposed machine is the first implementation of an encrypted manage device in the practical setting. Although we want more examination, the outcomes are useful to pick the appropriate key length.

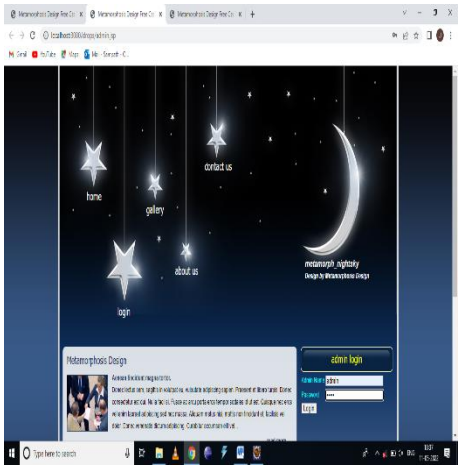


Figure 1: New admin

Web application to open admin new tab. Register your admin name and password.

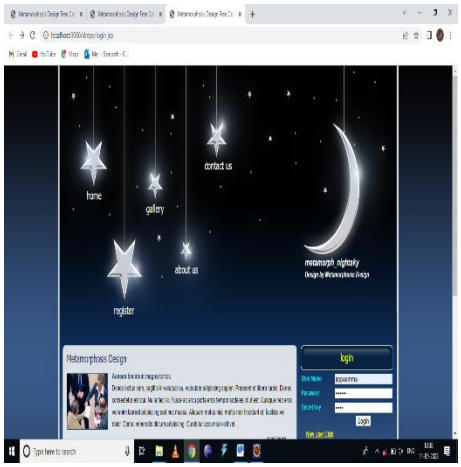


Figure 2: Login opening in new tab

Web application to open login new tab. register your user name, password and secret key.

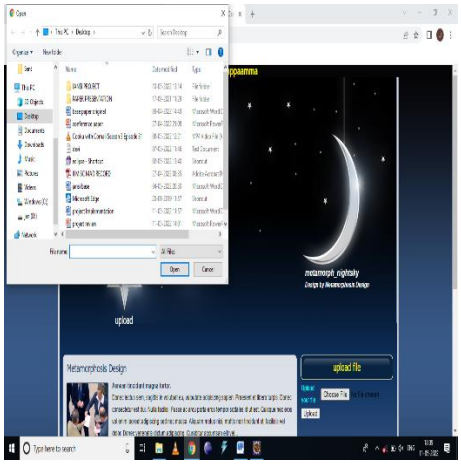


Figure 3: File Choosing

Choose in files to Text files, photos and pdf for all documents upload in web application.

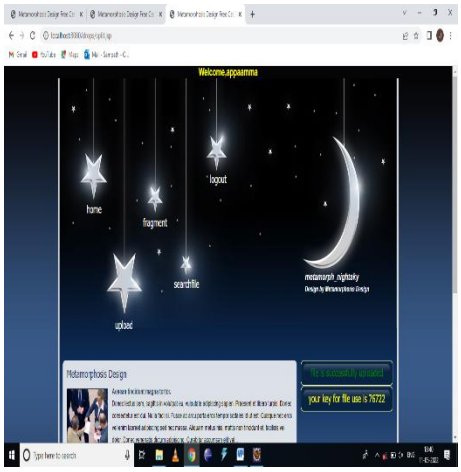


Figure 4: Uploading File

File uploaded. Each file we upload has a separate file key open. only with this file key can we view the file we uploaded.

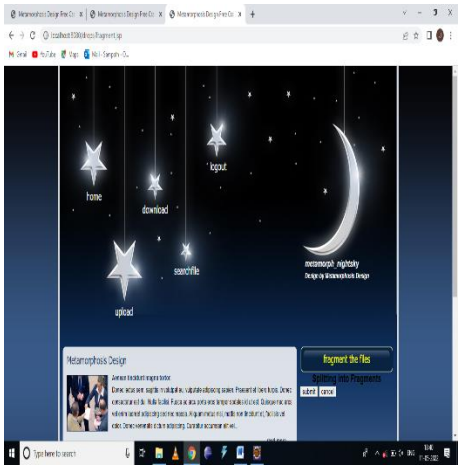


Figure 5: Uploading Files to fragment

Upload files to fragment. Fragments are into divided into many nodes to store in cloud.

Figure 6: Splitted Files into single fragment to store in cloud node

File is splitted into single fragments to store in cloud node.

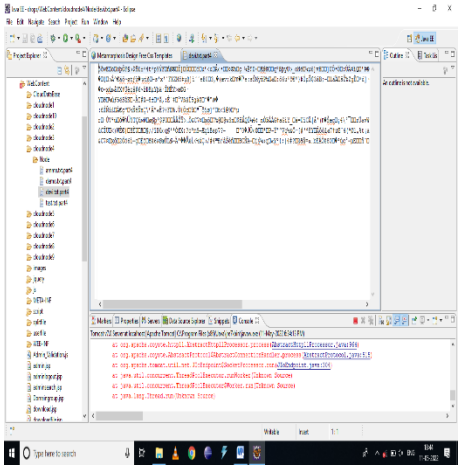


Figure 7: Uploaded files encrypted

Uploaded files can be protected by encryption. Encryption process to converts of the information, known as plaintext, into an alternative from known as cipher text. Encryption to use in security purpose.

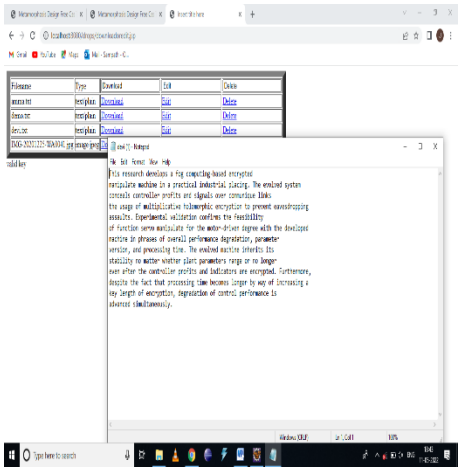


Figure 8: File Key

The original file is open to use the file key. To download the last file.

6. CONCLUSION

This paper develops a tightly closed fog computing-based control system, which serves as the first implementation of an encrypted control system in an actual industrial setting. The controller gains and alerts are hid against adversaries. The developed system is resilient to eavesdropping assaults and prevents zero dynamics attacks. Thus, the controller encryption technique can be employed as a new thing of protection in depth for industrial control systems. The experiment results affirm the feasibility of tracking control below load fluctuation and indicate the relationship between the key size and processing time. From the viewpoint of safety level and manage performance degradation, the key size need to be large. Therefore, the processes of encryption and decryption want to be implemented in the hardware (e.g., by means of a field programmable gate array) so that the encrypted manage systems can be put to sensible use in a more resource-limited setting. In future work, we will reflect on consideration on a fog computing-based control system with the cloud for higher-

layer control. Additionally, we will put in force an attack detection method to prevent DoS attacks, attain falsifications, and replay attacks.

7. REFERENCES

[1] M. S. Mahmoud and M. M. Hamdan, "Fundamental issues in networked control systems," IEEE/CAA J. Autom. Sinica, vol. 5, no. 5, pp. 902–922, 2018.

[2] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: Security and privacy issues," IEEE Internet Comput., vol. 21, no. 2, pp. 34–42, Mar./Apr. 2017.

[3] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in fog computing: A survey," Future Gener. Comput. Syst., vol. 88, pp. 16–27, 2018.

[4] K. Sato and S. Azuma, "Secure real-time control through fog computation," IEEE Trans. Ind. Informat., vol. 15, no. 2, pp. 1017–1026,Feb. 2019

[5] Y. Xia, "Cloud control systems," IEEE/CAA J. Automatica Sinica, vol. 2, no. 2, pp. 134–142, Apr. 2015.