

FLEXIBLE-EVENT TRIGGERED FILTER-DESIGN WITH RESTRAINT AND CYBER ATTACKS

SAIRAJ R¹, GOWRI V²

¹UG Scholar, Department of CSE, Kingston College, Vellore-59

²Asst. Professor, Department of CSE, Kingston College, Vellore-59

Abstract - Retaining cyber security in a constantly evolving risk panorama is a challenge for all companies. Traditional reactive techniques, wherein sources have been put towards protecting structures against the most important recognized threats, at the same time as lesser-known threats have been undefended, is not a enough tactic. To preserve up with converting security risks, a more proactive and adaptive method is necessary. One of the maximum complex factors of cyber security is the evolving nature of security dangers. As new technologies emerge are used in new or different approaches, new attack avenues are developed.

Retaining up with those common changes and advances in assaults, as well as updating practices to protect against them may be challenging. In this project the hybrid cyber-attack is investigated and handled in a way to secure the industrial level prototypes details securing. The new product details are always to be kept secured due to the confidential nature. Even many techniques were used hackers and other malicious persons uses techniques to get those data. If the attack happened in a hybrid way the handling of those things were proposed.

Key Words Traditional reactive techniques, security risks, hybrid cyber-attack,

1. INTRODUCTION

Retaining cyber safety in a continuously evolving hazard landscape is a project for all companies. Traditional reactive strategies, in which assets were placed toward protective systems in opposition to the maximum critical identified threats, on the equal time as lesser-acknowledged threats were undefended, isn't a sufficient tactic. To keep up with changing safety risks, a extra proactive and adaptive technique is necessary. One of the most complicated elements of cyber safety is the evolving nature of safety dangers. As new technology emerge are utilized in new or one-of-a-kind approaches, new assault avenues are developed. Retaining up with the ones not unusual place adjustments and advances in assaults, in addition to updating practices to defend in opposition to them can be challenging. In this undertaking the hybrid cyber-assault is investigated and dealt with in a manner to stable the economic degree prototypes information securing. The new product information are constantly to be saved secured because of the exclusive nature. Even many strategies have been used hackers and different malicious humans makes use of strategies to get the ones data. If the

assault came about in a hybrid manner the dealing with of these matters have been proposed.

2. RELATED WORKS

2.1 TITLE: Hybrid Event-Triggered Filtering For Nonlinear Markov Jump Systems With Stochastic Cyber-Attacks.

This paper studies the problem of H filtering for nonlinear Markov jump systems based on Takagi-Sugeno model. Firstly, we propose a hybrid event-triggered mechanism with an adjustable threshold, which not only helps to save more limited communication resources, but also excludes Zeno behavior while preserving the merits of continuous triggering. Secondly, given the threat of cyber-attacks to network security, a stochastic variable is introduced to describe the considered deception attacks in filter design. Thirdly, a less restrictive Lyapunov-Krasinski functional (LKF), which is not required to be continuous and positive definite in a triggering interval, is constructed to establish sufficient condition on the exponential mean-square stability for the filtering error system with a weighted H_∞ performance. Meanwhile, co-design of the desired filter and event-triggered mechanism is achieved. Finally, a tunnel diode circuit system is provided to illustrate the effectiveness and advantage of the obtained results.

2.2 TITLE: Event-Triggered Adaptive Fault-Tolerant Pinning Control For Cluster Consensus Of Heterogeneous Nonlinear Multi-Agent Systems Under Aperiodic Dos Attacks.

This paper presents an event-triggered cluster consensus scheme for heterogeneous nonlinear second-order multi-agent systems (MASs) subject to cyber attacks (i.e., aperiodic denial-of-service (DoS) attacks), actuator faults and integral quadratic constraints (IQCs) under directed communication topology containing a directed spanning tree. Based on local communication, an event-triggered adaptive fault-tolerant pinning control scheme is designed to achieve cluster consensus under simultaneous cyber attacks and actuator faults. The proposed control scheme does not require the communication topology to satisfy the in-degree balance between different clusters. Furthermore, the fault-tolerant control part only needs to estimate one parameter for each agent. Instead of requiring continuous information on its neighbors to determine the trigger instants as in the previous literature, an event-triggered mechanism that does not require periodic sampling of neighbors' information is developed to save network resources, and the Zeno behavior is excluded. Finally, a simulation example confirms the effectiveness and superiority of the proposed control scheme.

2.3 TITLE: Decentralized Resilient H_∞ Load Frequency Control For Cyber-Physical Power Systems Under Dos Attacks.

This paper designs a decentralized resilient H_∞ load frequency control (LFC) scheme for multi-area cyber-physical power systems (CPPSs). Under the network-based control framework, the sampled measurements are transmitted through the communication networks, which may be attacked by energy-limited denial-of-service (DoS) attacks with a characterization of the maximum count of continuous data losses (resilience index). Each area is controlled in a decentralized mode, and the impacts on one area from other areas via their interconnections are regarded as the additional load disturbance of this area. Then, the closed-loop LFC system of each area under DoS attacks is modeled as an aperiodic sampled-data control system with external disturbances. Under this modeling, a decentralized resilient H_∞ scheme is presented to design the state-feedback controllers with guaranteed H_∞ performance and resilience index based on a novel transmission interval-dependent loop functional method. When given the controllers, the proposed scheme can obtain a less conservative H_∞ performance and resilience index than the LFC system can tolerate. The effectiveness of the proposed LFC scheme is evaluated on a one-area CPPS and two three-area CPPSs under DoS attacks.

2.4 TITLE: An Improved Protocol To Consensus Of Delayed Mass With Unms And Aperiodic Dos Cyber-Attacks.

The present research focuses on the issue of leader-following consensus for multi-agent systems (MASs) suffered from uncertain nonhomogeneous Markov switching (UNMS), time-varying delay, and denial of service (DoS) cyber-attacks. Firstly, in contrast with the existing results on MASs, the communication topology is governed by a UNMS jump process in which the transition rates (TRs) of UNMS may be partially known or completely unknown. Secondly, the changes of communication topologies due to frequently aperiodic DoS cyber attacks are taken into consideration, which may destroy the chains of communication and lead to network paralysis in MASs. By introducing the concepts of average DoS ratio, novel mean-square leader-following consensus conditions which establish the relationship between control gains and sleeping, and active periods of DoS signal for MASs with the UNMS are proposed. It shows that there is no direct restriction on the time-varying delay of the system and the intervals between the sleeping period and the active period of the DoS jamming signal. Finally, the present theoretical result is validated by a numerical example.

2.5 TITLE: Probabilistic-Constrained H_∞ Tracking Control For A Class Of Stochastic Nonlinear Systems Subject To Dos Attacks And Measurement Outliers.

In this study, the probabilistic-constrained H_∞ tracking control problem is addressed for a class of stochastic nonlinear systems subject to measurement outliers, stochastic nonlinearities and DoS attacks. The considered systems have the following characters: 1) an unequal redundant-channel communication protocol is adopted to resist the DoS attacks and enhance the reliability of packet transmission. Different from some existing redundant-channel approaches, the considered two channels have different transmission abilities.

2) The measurement outliers (e.g., some unexpected large amplitude disturbances) are concerned and a saturation-function-based observer is proposed to avert the side effects from measurement outliers. 3) The DoS jamming attacks are considered in this paper, and an aperiodic DoS model is utilized. 4) Both sector-bounded nonlinear function and stochastic nonlinear function are involved in the considered systems, which makes the considered systems more general. To compensate the negative effect of the DoS jamming attacks and enhance the reliability of the packet transmission, a novel redundant-channel-based switching protocol is proposed to schedule data transmission when the plant suffers malicious cyber attacks. The primary objective of the present study is to design tracking controller such that the prescribed H_∞ control performance is reached and probabilistic constraints on the tracking error are satisfied simultaneously. To achieve this objective, a probabilistic-constrained H_∞ tracking control algorithm is established to obtain tracking controller gains and minimize the prescribed set of the constraint. Finally, two simulation examples are used to validate the practicability of our devised strategy.

2.6 TITLE: Fault Estimation And Fault-Tolerant Control For Networked Systems Based On An Adaptive Memory-Based Event-Triggered Mechanism.

This paper mainly focuses on the problem of networked fault estimation (FE) and fault-tolerant control (FTC). A novel adaptive memory-based mechanism is proposed by introducing the latest piece of historical output information. The historical information at each instant is matched with a corresponding weight such that the closer information is, the more contribution to the releasing event. Many unexpected triggering events can be avoided under this communication protocol, especially for the scenarios of the system with jitter disturbance or random noise. Moreover, to make the instantaneous data releasing rate adapt to the requirement of the control system, a time-varying threshold of the event-triggered mechanism is designed. Therefore, the burden of network bandwidth can be greatly decreased. Based on this proposed communication protocol, a new fault and state estimation model is developed. The fault-tolerant controller uses the estimations to compensate for the influence induced by the network and the fault. Sufficient conditions are derived to co-design the parameters of FE, FTC, and adaptive memory-based event-triggered mechanism. Finally, the performance of the proposed communication mechanism, FE, and FTC is evaluated on an example of the F-404 engine system.

2.7 TITLE: Bandwidth Allocation-Based Distributed Event-Triggered Lfc For Smart Grids Under Hybrid Attacks.

In this study, a bandwidth allocation-based distributed event-triggering load frequency control (LFC) has been developed for smart grids to deal with hybrid cyber-attacks, for example, denial-of-service (DoS) attacks and false data injection (FDI) attacks. Firstly, to prevent hybrid cyber-attacks from causing open-loop unstable operation of the LFC systems, we propose a distributed event-triggering communication (ETC) strategy. To attain the maximum usage of bandwidth, a dynamic bandwidth allocation mechanism is integrated with the ETC

approach on the basis of resource availability and error between the current state and equilibrium state. This bandwidth reservation and allocation approach aim at detecting attacks and assigning bandwidth to the different channels of distribution networks. Then, by virtue of the Lyapunov approach, the exponential stability criteria are established. Further, the exclusion of Zeno behavior of the designed systems is proved during the control process. Finally, comprehensive case studies show that the proposed method can improve the utilization rate of the network resource.

2.8 TITLE: A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges.

A cyber physical system (CPS) is a complex system that integrates sensing, computation, control and networking into physical processes and objects over Internet. It plays a key role in modern industry since it connects physical and cyber worlds. In order to meet ever-changing industrial requirements, its structures and functions are constantly improved. Meanwhile, new security issues have arisen. A ubiquitous problem is the fact that cyber attacks can cause significant damage to industrial systems, and thus has gained increasing attention from researchers and practitioners. This paper presents a survey of state-of-the-art results of cyber attacks on cyber physical systems. First, as typical system models are employed to study these systems, time-driven and event-driven systems are reviewed. Then, recent advances on three types of attacks, i.e., those on availability, integrity, and confidentiality are discussed. In particular, the detailed studies on availability and integrity attacks are introduced from the perspective of attackers and defenders. Namely, both attack and defense strategies are discussed based on different system models. Some challenges and open issues are indicated to guide future research and inspire the further exploration of this increasingly important area.

2.9 TITLE: Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks

This article focuses on the issue of decentralized event-triggered synchronization control for complex networks (CNs) under nonperiodic denial-of-service (DoS) attacks. First, to alleviate the pressure on network bandwidth, a decentralized event-triggered scheme is employed at each coupled node to decide whether the synchronization signal is transmitted to the communication network. Then, an event-based synchronization error model is established for CNs under DoS attacks, where the communication network is assumed to be composed of multiple transmission channels and DoS attacks will independently compromise each of channels. Based on the constructed model, sufficient conditions that assuring the secure synchronization of the system are analyzed with the assistance of Lyapunov stability theory. Meanwhile, the synchronization controller gains are designed by solving a set of linear matrix inequalities. The efficiency of the study is finally validated by simulations.

2.10 TITLE: Event-Triggered Formation Tracking Control for Unmanned Aerial Vehicles Subjected to Deception Attacks.

This study investigates the time-varying formation tracking (TVFT) control problem for multiple unmanned aerial vehicle

(multi-UAV) systems under deception attacks by utilizing an event-triggered mechanism (ETM). First, for the sake of alleviating the communication burden, an effective ETM is designed in this paper. Second, to deal with deception attacks in the communication network, a random deception attack model under the designed ETM is constructed. Finally, a novel formation tracking control scheme for multi-UAV systems under deception attack combining the ETM is proposed to achieve the expected TVFT. The stability analysis of the formation control system is given by using the Lyapunov stability theory and linear matrix inequality (LMI) technique. Simulations are conducted to verify the effectiveness of the proposed formation control scheme.

3. PROPOSED SYSTEM

The proposed machine can correctly manipulate the personal statistics to be shared among the primary entities like company, Manufacturing unit, Admin and employees. Every statistic isn't always absolutely to be had for each person for production the prototypes. At the equal time all of the shared and the producing statistics to be saved at the database, an powerful mechanism will take care of the hybrid assault from the malfunctioning of the statistics. It has the blessings of handy statistics aid sharing, fewer connections, easy set up and maintenance, low cost, etc.

3.1 MERITS OF PROPOSED SYSTEM

- Achieved malicious reduced data sharing.
- Secured data from hybrid attacks.
- Maintenance and management of data made simpler.
- Authorized entities only have proper access to data.

3.2 MODULES DESCRIPTION

Company

In this module company user register and login their details. After that company users enter their prototype details based on customized module, then decryption key also generated, Then the xml file has been generated for that required specification which has been shown in a tabular format. The generated xml file has send to the admin and the status is also updated, for verification and starting the production. After that the company user has logged out from that module.

Employee

In this module employee register their details and login to the module, the employee view and ordered the prototype with that work update the employee finishing status, After that employee logout from their module

Admin

In this module admin login with their password, Then it has been redirected to the admin home page, which contains employees, specification data, loading data. The employees menu which contains employees register details that has been monitor by admin, and specification data menu which contains id, date, name, status , message. Then download the prototype specification in an encrypted format from the employee creation and updating its status. Then admin load

the encrypted data and enter the corresponding key values, decrypted the details and delivery date and time has been updated. Once it has been done then the details has been send to the manufacture team to start manufacturing.

Hacker

In this Hacker Page which contains the list of commands, Then admin will connect with its server if the hacker has been connected then the data has been engaged and accessing the with its database. After that hacker has accessed then file and its decryption key has been retrieved from database

4.ARCHITECTURAL AND DATA FLOW DIAGRAM

4.1 SYSTEM ARCHITECTURE

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development.

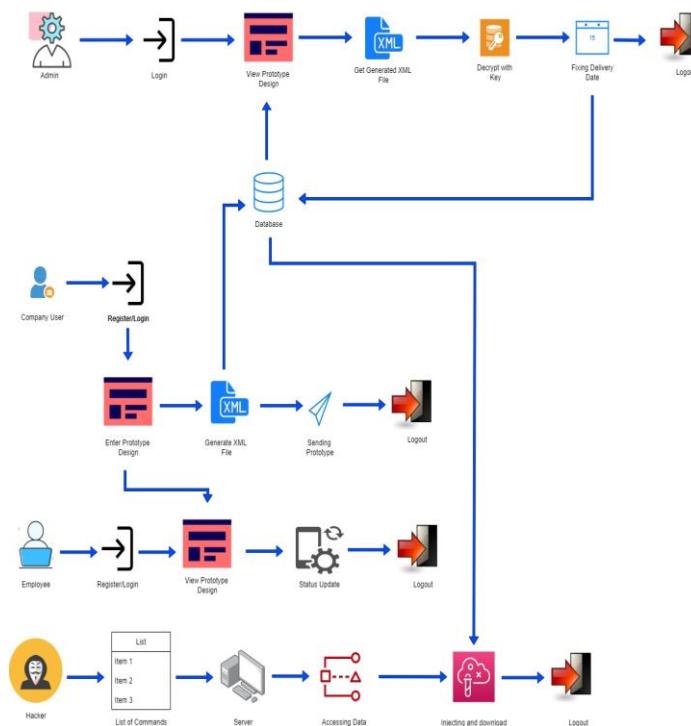


Figure 1: System Architecture

4.2 DATAFLOW DIAGRAM

A data flow Diagram is a graphical representation of the through an information system, modeling its process aspects often used as a preliminary step to create an overview of the going into great detail, which can later be elaborated.

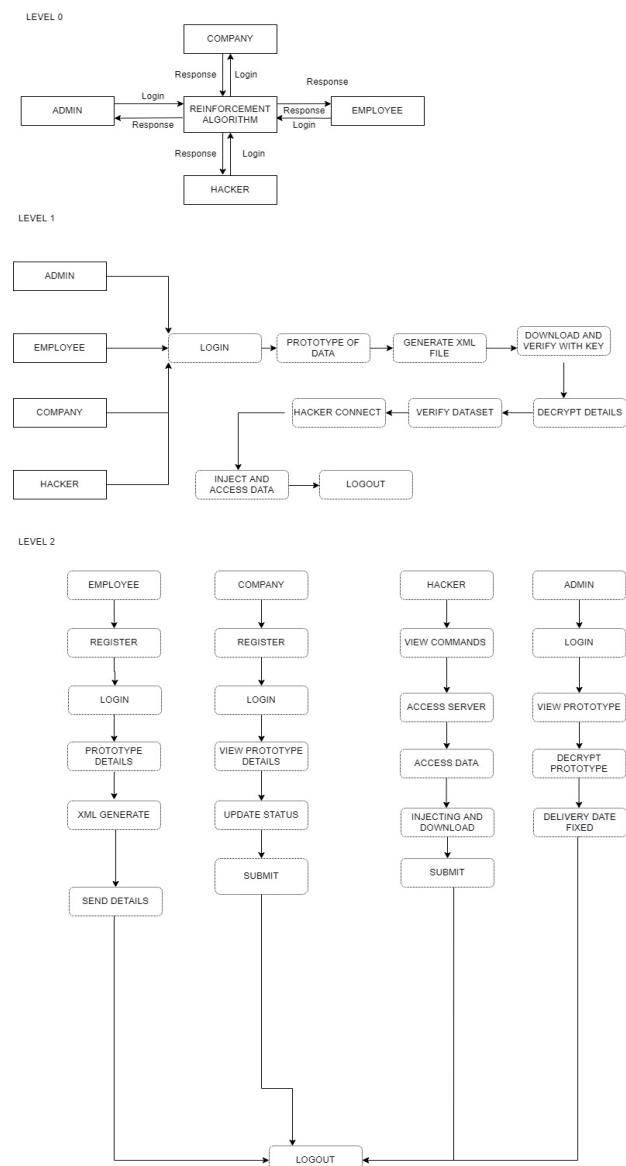


Figure 2: Dataflow Diagram

4.3 OTHER DIAGRAM

4.3.1 USE CASE DIAGRAM

Use case diagram is a graphic depiction of the interactions among the elements of a system. Use cases will specify the expected behavior, and the exact method of making It happened. Use cases once specified can be denoted both textual and visual representation.

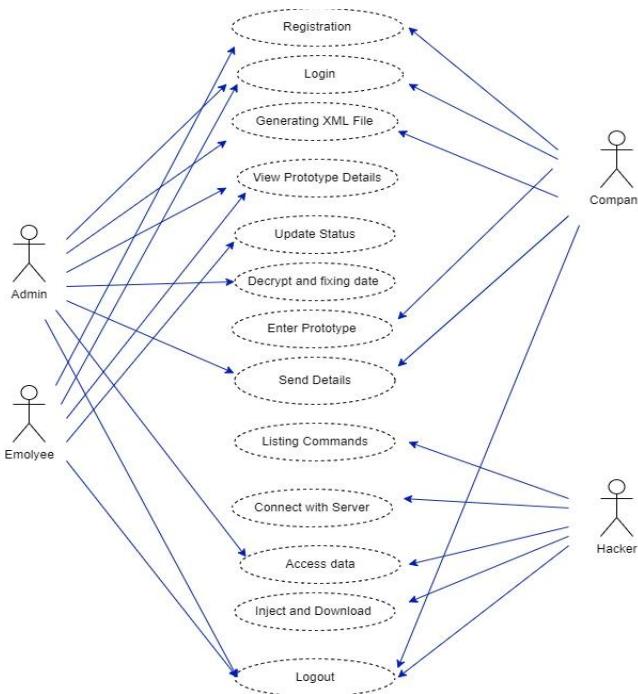


Figure 3: Use Case Diagram

5. RESULTS AND OBSERVATIONS

The system worked well efficient in different scenarios.

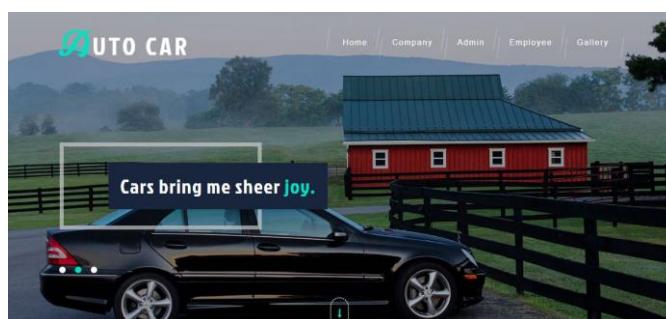


Figure 4: Landing Page

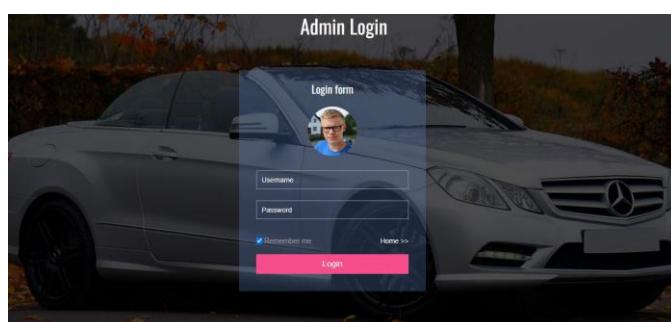


Figure 5: Admin Page

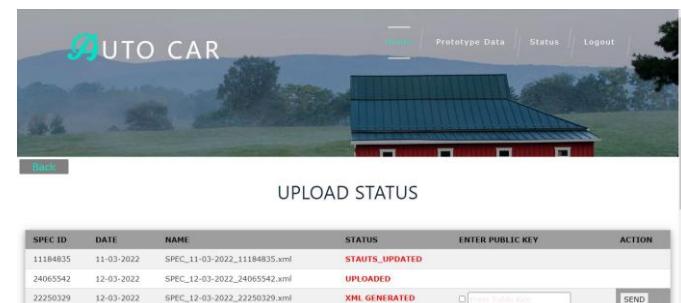


Figure 6: Upload status



Figure 7: Xml Details



Figure 8: Prototype Specification

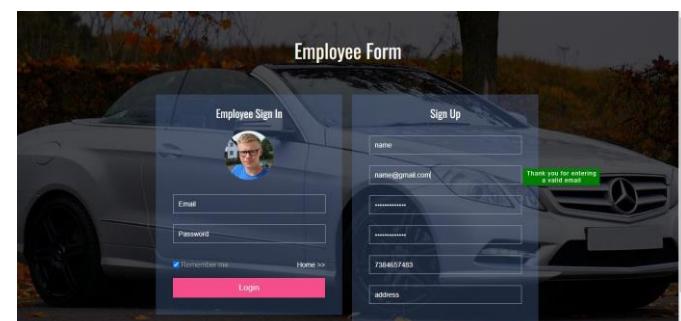


Figure 9: Employee From page

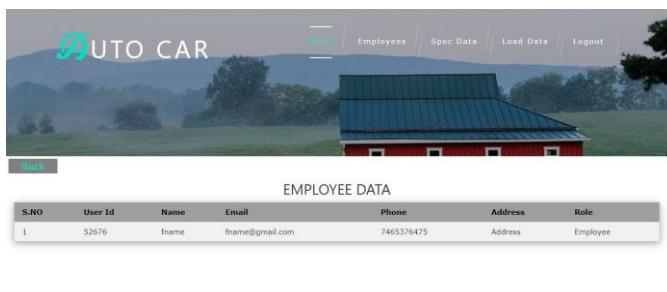


Figure 10: Employee Data

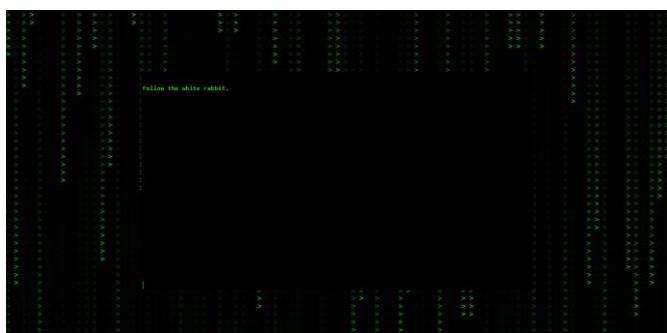


Figure 11: Key Page

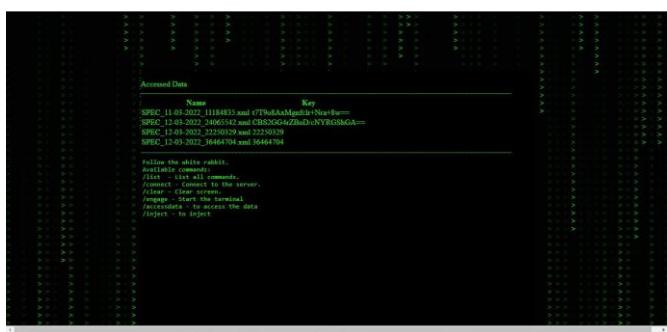


Figure 12: Key Verification Page

6. CONCLUSION

The at ease adaptive-event-precipitated filtering with hybrid cyber-attack and input constraints are investigated and implemented in an Organizational data sharing platform. To save the restrained network and power resources, and the adaptive occasion-prompted scheme is delivered. Then, by using taking the influence of the hybrid cyber assault into account, a unique filtering errors version with the adaptive scheme and input constraint is hooked up. Sufficient conditions to assure the system balance is received. The demand in the automotive sector is increasing as the automakers have begun investing more in this industry.

The capability of the methodology in assessing little volumes inside allowable state spaces in information driven way and the basic preferred position of without model set assessment is shown exactly. We additionally represent how one could utilize this strategy to choose solvers for no convex improvement issues by dividing the achievable area of the

solvers. In future it has been enhanced and applied with experimented for an effective needed situation.

ACKNOWLEDGEMENT

The authors would like to thank Mrs.V.Gowri for her suggestions and excellent guidance throughout the project period.

REFERENCE

- [1] Wenqian Xie, Yong Zeng, Kaibo Shi, Xin Wang, Qianhua Fu, "Hybrid Event-Triggered Filtering for Nonlinear Markov Jump Systems With Stochastic Cyber-Attacks", IEEE Access, vol.9, pp.248-258.
- [2] Xiang-Gui Guo, Pei-Ming Liu, Jian-Liang Wang, Choon Ki Ahn, "Event-Triggered Adaptive Fault-Tolerant Pinning Control for Cluster Consensus of Heterogeneous Nonlinear Multi-Agent Systems Under Aperiodic DoS Attacks", IEEE Transactions on Network Science and Engineering, vol.8, no.2, pp.1941-1956.
- [3] Xin Zhao, Suli Zou, Zhongjing Ma, "Decentralized Resilient H_∞ Load Frequency Control for Cyber-Physical Power Systems Under DoS Attacks", IEEE/CAA Journal of Automatica Sinica, vol.8, no.11, pp.1737-1751.
- [4] Xin Wang, Ju H. Park, Huilan Yang, "An Improved Protocol to Consensus of Delayed MASs With UNMS and Aperiodic DoS Cyber-Attacks", IEEE Transactions on Network Science and Engineering, vol.8, no.3, pp.2506-2516.
- [5] Bin Wei, Engang Tian, Tao Zhang, Xia Zhao, "Probabilistic-Constrained H_∞ Tracking Control for a Class of Stochastic Nonlinear Systems Subject to DoS Attacks and Measurement Outliers", IEEE Transactions on Circuits and Systems I: Regular Papers, vol.68, no.10, pp.4381-4392.
- [6] Zhou Gu, Peng Shi, Dong Yue, Shen Yan, Xiangpeng Xie, "Fault Estimation and Fault-Tolerant Control for Networked Systems Based on an Adaptive Memory-Based Event-Triggered Mechanism", IEEE Transactions on Network Science and Engineering, vol.8, no.4, pp.3233-3241.
- [7] Md Musabbir Hossain, Chen Peng, Hong-Tao Sun, Shaorong Xie, "Bandwidth Allocation-Based Distributed Event-Triggered LFC for Smart Grids Under Hybrid Attacks", IEEE Transactions on Smart Grid, vol.13, no.1, pp.820-830.
- [8] Wenli Duo, MengChu Zhou, Abdullah Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges", IEEE/CAA Journal of Automatica Sinica, vol.9, no.5, pp.784-800.
- [9] Yan Li, Feiyu Song, Jinliang Liu, Xiangpeng Xie, Engang Tian, "Decentralized event-triggered synchronization control for complex networks with nonperiodic DoS attacks",

International Journal of Robust and Nonlinear Control, vol.32,
no.3, pp.1633.

[10] Biao Sun, Zhou Gu, Tianyi Xiong, "Event-Triggered Formation Tracking Control for Unmanned Aerial Vehicles Subjected to Deception Attacks", Electronics, vol.10, no.22, pp.2736.

[11] Jinyong Yu, Mengmeng Liu, Juan J. Rodríguez-Andina, "Zonotope-Based Asynchronous Fault Detection for Markov Jump Systems Subject to Deception Attacks via Dynamic Event-Triggered Communication", IEEE Open Journal of the Industrial Electronics Society, vol.3, pp.304-317.