JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security Design for Face Recognition in Embedded Device

Nirmala Dahal[1], Priya N[2]
[1]*Final Year PG Student, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru*
[2]*Professor, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru*
Email: neerudahal4@gmail.com[1], n.priya@jainuniversity.ac.in[2]

ABSTRACT: IoT will allow objects and machines to connect and communicate with the presence of the internet. In IoT, specific sensors are attached to every embedded device to capture information from the physical world. Unauthorized access has increased drastically in IoT devices with the increase in IoT use. This project will be focusing more on security and prevention of unauthorized access in the application layer of different devices. IoT will allow objects and machines to connect and communicate with the presence of the internet. This project will be focusing more on security and prevention of unauthorized access in the application layer of different devices.

Keywords: ***IoT, Authentication, Raspberry Pi, Face-Recognition, unauthorized access***

I. INTRODUCTION

An embedded system that represents the connection of physical objects that are a set of software tools, hardware resources, sensors, and other technologies for the transfer of data and information with other electronic devices and embedded systems over the internet is called IoT. The embedded devices can be ordinary household devices or multi-million-dollar industrial tool which is used in the market. A decade ago, IoT devices have got immense importance in different industrial sectors. Now that we can connect everyday objects like kitchen appliances, security scanning, face recognition, fingerprint, cars, thermostats, baby monitors, etc. through the internet via embedded devices, seamless communication is possible between people, processes, and things. With very low-cost computing, big data, cloud, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention. In this hyperconnected world, digital systems can record, store, monitor, and adjust each interaction between different connected things. With the help of IoT, the physical world interacts with the digital world and they cooperate. Security has been designed as a process of protecting an object against physical damage, unauthorized access, theft, or any other threads which can affect organizations or individuals, by maintaining high confidentiality and integrity of information about the object and making information secure, and providing object available whenever needed. Several things such as low cost in hardware and network infrastructure and the rapid development of wireless communication technologies enabling quick and easy deployments are leading to the development of emerging scenarios creating effective experiences for people and affordable economic and social opportunities for companies, individuals, and countries. The security aspect of an IoT plays a most important role in the different ways of authentication with the help of a sensor. Security has become stronger and user friendly. The authentication is being used in office

attendance, Door lock, security alert, fire alert, military, and many more. In each aspect of security, they have used Sensor, Raspberry PI, and Raspberry PI camera. The development of an IoT still found different security issues in different phases of the development of an IoT.

II. Related Work

This project "Security Framework for Preventing Unauthorized Access in IoT**"** is implemented to enhance security in IoT devices. The rapid growth in the field of the Internet of Things (IoT) and it is very convincing potential to resolve different types of the problem by using numerous services have made it the quicker growing technology, with more effect on social lifestyle and enterprise environments. IoT has made everything modern, such as education, healthcare, and enterprise, involving the storage of sensitive information about individuals and companies, financial data transactions, product development, and marketing of human life.

Following are the finding of the research papers:

1. "In the Paper "Fault Tolerance Mechanisms into the Military IoT by Zbigniew Zieliski, Jan Chudzikiewicz, and Janusz Furtak - 2019" the Authors pointed out that security methods and uninterrupted strategies to be powerful in military applications should be tightly integrated. In this paper, the author analyses solutions for securing the military IoT network, ensuring strong nodes authentication within a network, and securing data transmissions among sensor nodes and gateways.
2. Secure IoT Supply Chain Management Solution Using Blockchain and Smart Contracts Technology-Cristian Toma, Bogdan Talpiga, Catalin Boja, Marius Popa, Bogdan Iancu, Madalina Zurini – 2019. Due to the globalization effects has on the world economic system. The study of the combination creates the knowledge and the infrastructure wished for the networks of an interdependent group of organizations, that allow them to provide a more dynamic demand and supply of products and services. The paper presents a solution by using the blockchain and smart contracts technologies within IoT – Internet of Things environment and provide a more dynamic demand and delivery of products and services
3. The author of the paper name "Countering the IoT-Powered Volumetric Cyberattacks with subsequent technology Cyber-Firewall" has defined approximately the cyber-attack are stated by using the Internet of Things (IoT) are inflicting major damage and it has led to a signified negative impact on critical infrastructures, such as electricity, telecommunication, and water supply. The proposed firewall offers deep packet inspection featurization vest iGATE the incoming network drift and distinguishes benign and malicious network traffic.
4. 4. Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox, and NB-IoT by Florian Laurentiu Coman, Krzysztof Mateusz Malarski, Martin Nordal Petersen and Sarah Ruepp -2019. The aspect of the communication security mechanism remains the least matter, even though the potential harm of a powerful hacker attack can be harmful. This paper describes and analyzes the LP-WAN vulnerabilities and several Proof-of-Concept attacks toward Lora WAN Sigfox (replay with DoS) and NB-IoT (attack using malicious UE) to confirm the existence of the vulnerabilities in both the standards and off-the-counter hardware and services.
5. IoT-based hydroponics system using Deep Neural Networks Manav Mehra, Sameer Saxena, Suresh Sankar Narayanan, Reijo Jackson Tom, M. Veera Manikandan – 2019. This work proposes to develop a smart IoT-based aquiculture system by emerging Deep Neural Networks which is the first of its kind to gather the system so developed is intelligent enough in providing the appropriate control action for the hydroponic environment based on the multiple-input parameter. Agriculture has the most impact on the country's economy with the practice of modern farming techniques where plants can be grown without the need for soil or a natural resource, Hydroponics and Aeroponics are in the demand in this changing world.
6. Use of blockchains for secure binding of metadata in military applications of IoT by Konrad Wrona, Michal Jarosz – 2019. In this paper, the author discusses how blockchain can be used to store metadata describing information collected from the IoT devices owned by the federation members as well as crowdsourced from sensors belonging to private users. This paper briefs the details and the idea behind, the creation of a Python wrapper for SRUP and describes a worked example of usage. The Secure Remote Update Protocol provides the technology that makes the possible formation of secure messages for transmission using similar techniques.
7. syrupRUP-Simplifying secure Communications for Command and Control in the Internet of Things by Andrew John Poulter, Steven J. Johnston, Simon J. Cox – 2019. The device's connection is a part of the Internet of Things, and other connecting

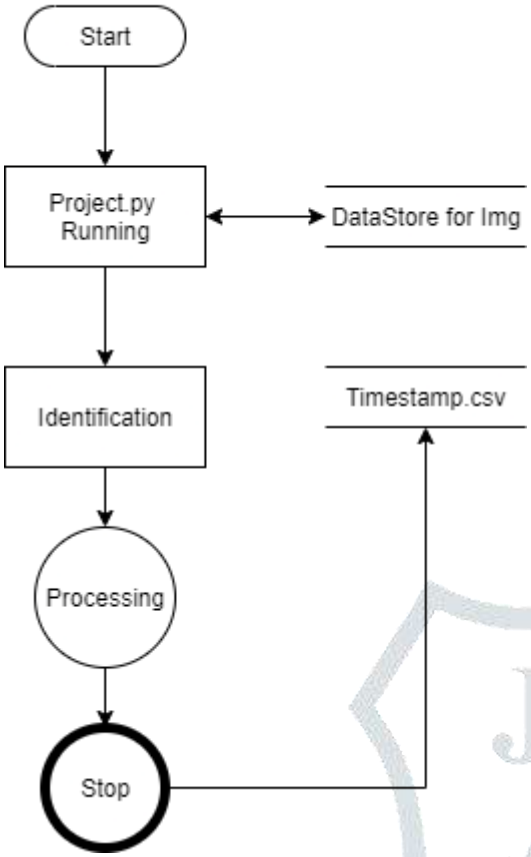
devices, require a secure technique to incorporate the propagation of Command-and-Control messages to enable the remote management of the devices. In this paper, the authors explained the details and purpose behind the creation of a Python wrapper for SRUP: and describe a worked process and an example of usage. The Secure Remote Update Protocol (SRUP) provides a technique to facilitate the development of secure messaging transferring using common techniques.

8. Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD by Md Iman Ali, Sukhkirandeep Kaaur2, Aditya Khamparai, Deepak Gupta, Sachin Kumar, Ashish Khanna- 2020 Environment. In BYOD it increased the significant risk of the cyber-attack which is leading to a major reason for business disruption and becomes a leading question about how to get a cybercrime secured citizenship in the smart city where crime takes place every second as well as in the organization where BYOD is used in large numbers. To process and implementation of various forensic investigation incident detection and risk management of different malicious activities from IoT/BYOD endpoint is a complex task to do. An impAn impending crisis in BYOD cyber forensic ecosystem is a unique mechanism of detection of malicious activities which is a core component. Detecting suspicious activities was in requirement to build an advanced technique in this trending world. This paper focused on a new abstraction with a more useful technique in some approaches for detecting various malicious activities in a BYOD environment. Ending crisis in BYOD cyber forensic
9. Comparison of three CPU core families for IoT applications in terms of security and performance of AES-GCM by Yaroslav Sovyn, Volodymyr Khoma, and Michal Podpora -2019. Although various parts of the development of the AES-GCM for high-end processors and hardware were examined briefly. The main goal of the proposed system was to achieve the maximum speed and accuracy, as well as to ensure a constant time of the algorithm implementation during encryption and decryption is the main aspect in the protection against Side-Channel Attacks.
10. A review of IoT Architecture, Technologies and Smartphone-based attacks against 3D printers by Muhammad Bila – 2019. The security issues in the IoT perception layer are a fake node, malicious code injection, protecting sensor data, mass code authentication, physical damage, and node tempering issues. The IoT devices have a various vision that provides different services, services as earthquake monitoring systems, building monitoring systems, landslides detection, energy management, property management, air quality noise monitoring system, etc.

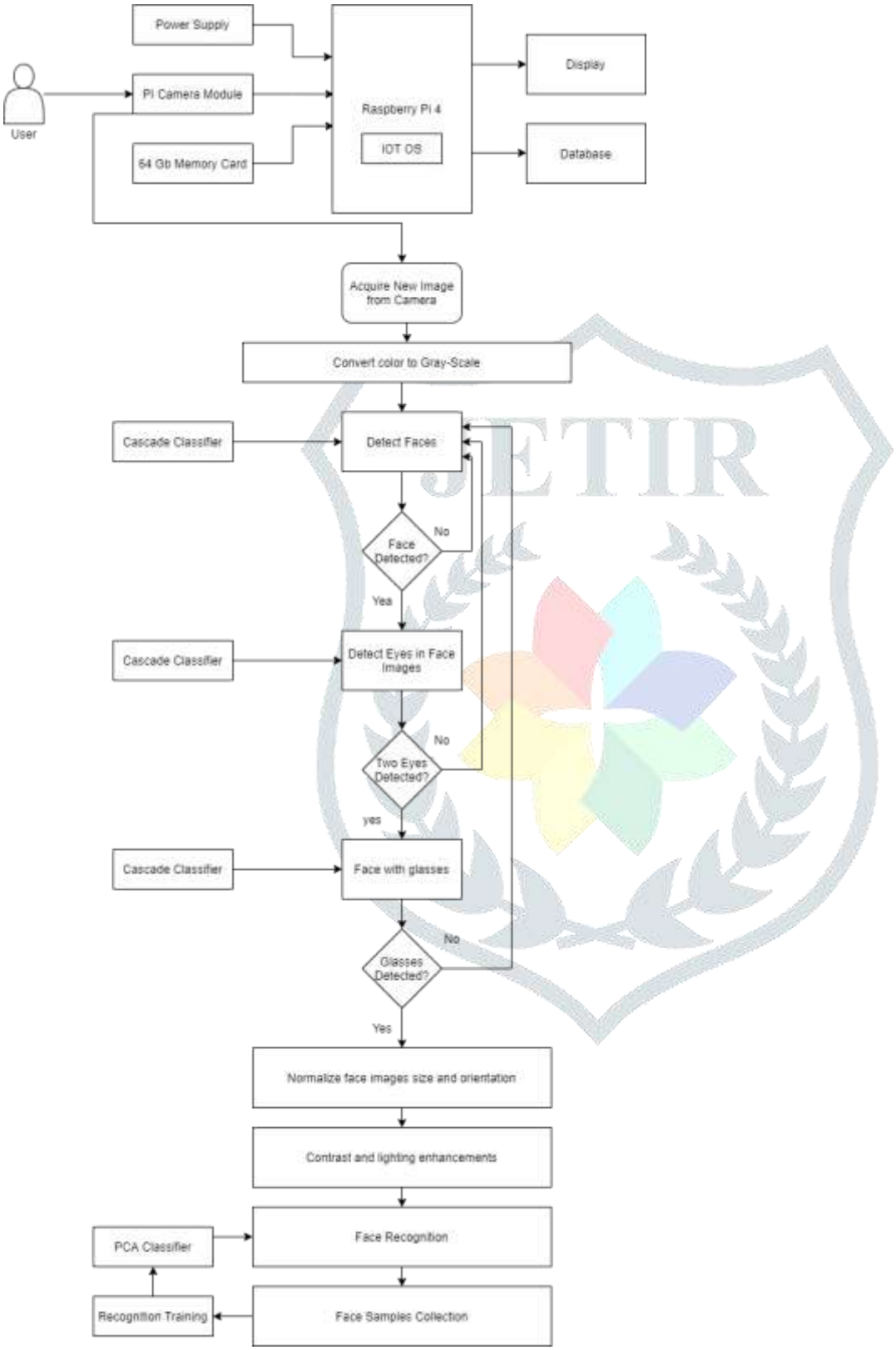
III. Proposed System

Dataflow Diagram: Dataflow diagram shows the flow of the data, from one component to the other component. In the proposed system the flow starts from the stored directory where all the photo data for each authorized user is stored. After the pictures are encoded. The system turns on (Note: If you are running an anti-virus that checks abnormalities with the hardware, I suggest turning it off). The camera turns on and authenticates the user. Once the system is turned off the timestamp is stored in the time.csv file.

Software Part of the Proposed system



Flowchart Diagram: Consisting of every part of the system and showing the flow of the control of the data from the start till the end part. Consisting of every part of the system.



IV. Results and Discussion:

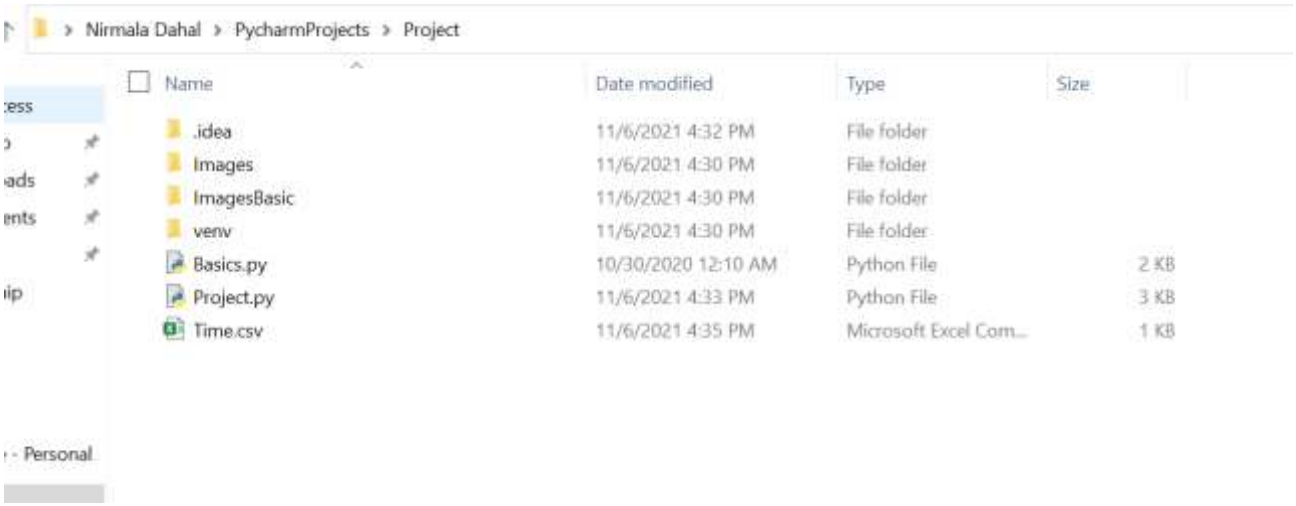


Fig 1: Directory of the Project

The directory of the Proposed system consists of a folder by the name images which contains all the authorized users' Images. Which will be encoded before the system runs.

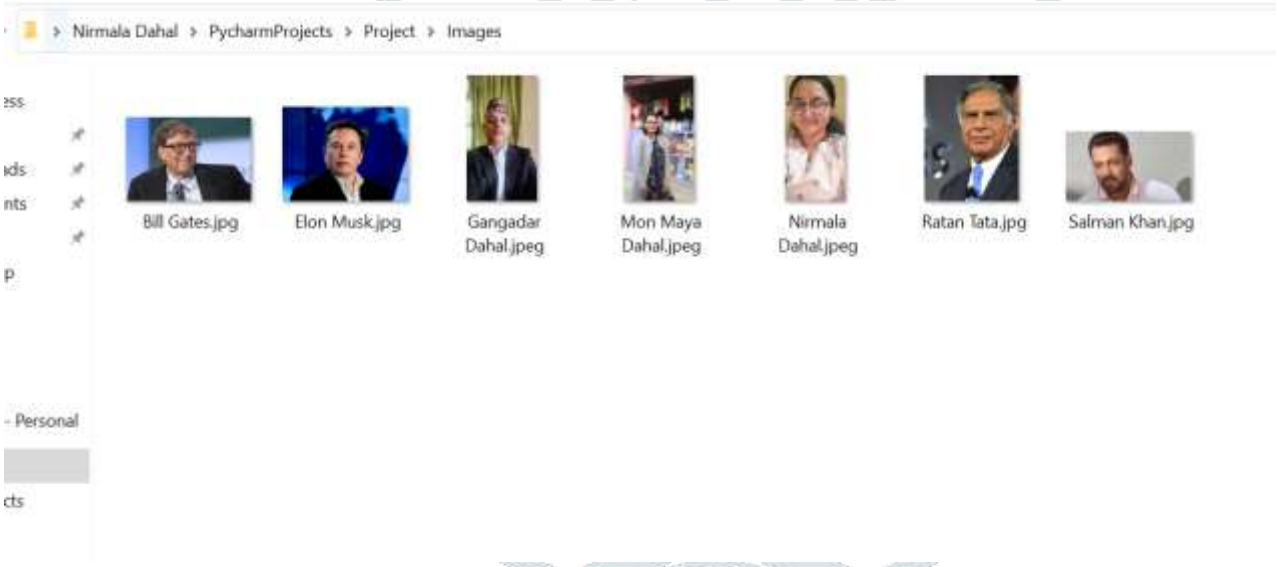


Fig 2: test image

All the test images of the system are very essential for the identification of the faces.

```
C:\Users\neeru\AppData\Local\Programs\Python\Python39\python.exe C:/Users/neeru/PycharmProjects/FaceRecognizationProject/Project.py
['Bill Gates.jpg', 'Elon Musk.jpg', 'Gangadar Dahal.jpeg', 'Mon Maya Dahal.jpeg', 'Nirmala Dahal.jpeg', 'Ratan Tata.jpg', 'Salman Khan.jpg']
['Bill Gates', 'Elon Musk', 'Gangadar Dahal', 'Mon Maya Dahal', 'Nirmala Dahal', 'Ratan Tata', 'Salman Khan']
Encoding Complete
```

Fig 3: Encoding the Images

All the images are encoded before the system starts.

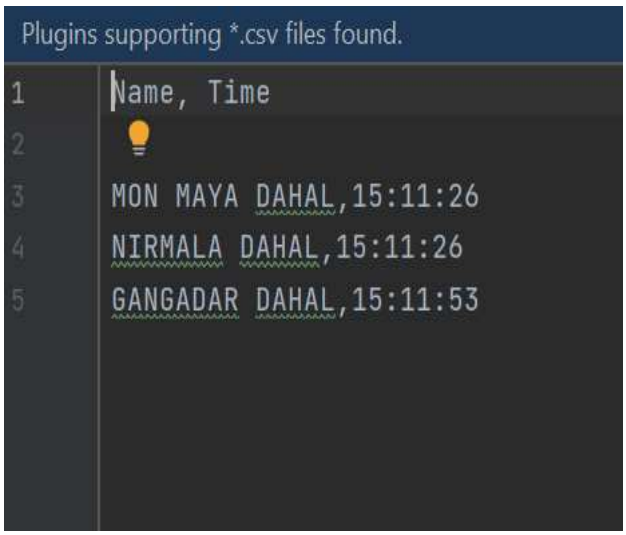


Fig 4: logs of users with Timestamp

The timestamps are successfully saved in the file

Fig 5: Outcome of the system

The System works with high accuracy.

V. CONCLUSION AND FUTURE ENHANCEMENT

With the development of IoT and its different systems, data breaches, threats, and attacks have rapidly increased. Many such risks and attacks are attributable to devise vulnerabilities that arise from different cybercrime performed by hackers and unauthorized use of system resources. The IoT system needs to be built in such a manner as to ensure easy and safe and secure usage control. People need to trust fully and embrace the IoT to utilize its benefits and avoid security and privacy risks and attacks. IoT faces several threats, risks, and attacks that must be recognized and mitigated to protect and stop future risks and threats. So, keeping in mind the security perspective, the work has been enforced to make a system more secure and authenticated using face recognition. Once the face got scanned the login will be stored in the database with the details of the user, date, and time to authenticate and authorize the user.

VI. REFERENCES

- Zbigniew Zieliski, Jan Chudzikiewicz and Janusz Furtak "An Approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT" 2019
- Cristian Toma, Bogdan Talpiga, Catalin Boja, Marius Popa, Bogdan Iancu, Madalina Zurini "Secure IoT Supply Chain Management Solution Using Blockchain and Smart Contracts Technology" -2019
- Arif Sari- "Countering the IoT-Powered Volumetric Cyberattacks with Next-Generation Cyber-Firewall: Seddulbahir" 2019
- Florian Laurentiu Coman, Krzysztof Mateusz Malarski, Martin Nordal Petersen and Sarah Ruepp "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox, and NB-IoT" - 2019
- Manav Mehra, Sameer Saxena, Suresh Sankaranarayanan, Rijo Jackson Tom, M. Veeramanikandan "IoT based hydroponics system using Deep Neural Networks" -2019
- Konrad Wrona, Michał Jarosz- "Use of blockchains for secure binding of metadata in military applications of IoT" 2019
- Andrew John Poulter, Steven J. Johnston, Simon J. Cox -2019 " pySRUP – Simplifying Secure Communications for Command & Control in the Internet of Things"
- Md Iman Ali, Sukhkiran Deep Kaur2, Aditya Khamparia, Deepak Gupta, Sachin Kumar, Ashish Khanna "Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment" -2020
- Yaroslav Sovyn, Volodymyr Khoma, and Michal Podpora "Comparison of three CPU-core families for IoT applications in terms of security and performance of AES-GCM" -2019
- Muhammad Bila "A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers" -2019