Cyber Physical Systems Security
Limitations, Issues and Future Trends

American University of Beirut
Cybersecurity Research Group
Cybersecurity Research Group

Professor Ali Chehab

Associate Professor Rouwaida Kanj

Research Scientist and Lecturer Dr. Hassan Noura
Biography: Rouwaida Kanj

2012-present
American University of Beirut (Lebanon), Associate Professor of Electrical and Computer Engineering

Research Interests and Projects: Advanced algorithmic research and smart Analytics for Design for reliability and yield, Machine learning for VLSI, Smart Grid Security, and Medical Devices.

2004-2012
IBM Austin Research Labs, Research Staff Member

1998-2004
UIUC (PhD 2004, MSc 2000)
SOI Circuit Design Styles and High-Level Circuit Modeling Techniques, Adviser: Prof. Elyse Rosenbaum (recipient of 3 IBM PhD fellowships)
High Level Design Exploration and Optimization, Adviser: Prof. Farid Najm (now @ UToronto)

1994-1998
American University of Beirut, (BEng, 1998)

Awards: holder of 6 invention plateau awards, outstanding technical achievement award, 3 best paper awards
A Glimpse on Cyber Physical Systems
Rapidly Changing World

• World’s population is growing: 7 billion and counting
• Resource consumption is increasing dramatically: Annual per capita energy consumption at about 20 MWh/year
• At the same time, advances in the communication and computation infrastructures are happening at a fast rate
• Need to leverage advances in science and technology to help us influence the world for better sustainability and growth

ztrela.com/images/nnc.png

Cybernetics: Science for Military Purposes

• During WWII, Norbert Wiener pioneered technology for the “automatic aiming and firing of anti-aircraft guns”

• The term “Cybernetics” was coined by Wiener who had significant impact on control theory

"cybernetics" = kybernetes (greek)= Pilot

• Although he had no computers, the principles involved are similar to those used today in a huge variety of computer-based feedback control systems

• Considered as the beginnings for Cyber Physical Systems

Cyber Physical Systems

• Introduced in 2006 by Helen Gill at the National Science Foundation

• CPS is about the integration of physical and cyber for enhanced control and operation
  • Cyber components = computation and communication
  • Physical components = sensing and actuation

• It’s all about understanding the joint dynamics of computers, software, networks, and physical processes

CPS applications

- CPS affects various aspects in people's way of life and enables a wider range of services and applications.

- Cyber-physical systems include:
  - Industrial automation systems and robots,
  - Vehicular systems (e.g.: collision avoidance, autonomous driving),
  - Transportation systems (e.g.: traffic management, airports, etc.),
  - Medical systems (e.g.: integrated diagnostics and medication, remote surgery)
  - Power systems (e.g.: load balancing between demand and supply)
  - Smart cities, buildings and homes (e.g.: cooling, lighting, access)

"Entire planet as a single, massive Cyber-Physical System"
Cyber Physical Systems (CPSs)

• Heterogeneous and require novel methods and tools to function
• Operate in a *dynamic environment*
• *Adaptation* and *self-learning* are necessary features to ensure reliable and fault tolerant operation
• *Control critical infrastructures*
• Therefore, they entail incredibly *high security requirements*

Risks of Complex Cyber Physical Systems

• CPSs are subject to serious risks
• The use of complex cyber-physical systems in today’s airplanes has redefined “the aerospace cybersecurity paradigm”
• There is a need to
  • Mitigate or prevent cyber attacks on communication and navigation systems
  • Enhance passengers’ safety

https://www.semanticscholar.org/paper/A-Systems-Engineering-Approach-To-Appraise-Risks-Of-Bogoda-Mo/1e54a67a176a1cbb62b6ff35f8699d817f58307

Cyber Security Research Group
Security Costs

1. IT Security spending $101 billion in 2018
2. IT Security will hit $170 billion by 2020
3. Avg-Time (Breach & Detection) 205 days
4. 90 million cyber attacks annually
5. Cost of data breach hitting $2.1 trillion globally by 2019

Cost Of Security

Cost around $575 billion

Cybersecurity Research Group
Too much to Gain, Too much at stake!

https://whatismyipaddress.com/wireless-hacking
Let’s connect the dots...

https://www.tap.io/app/2176
Outline

1. CPS – Background
   - CPS Layers
   - CPS Use & Classification
   - CPS Components

2. CPS Security Alert
   - CPS Threats
   - CPS Vulnerabilities
   - CPS Attacks
   - CPS Challenges

3. CPS Security Measures
   - CPS Risk Management
   - Cryptographic Solutions
   - Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: Cyber Security and AI
Introduction

• Cyber-Physical Systems include:
  o Real-time, embedded and/or transactional services systems
  o Possible communication between system components

• Cyber and physical processes collaborate with each other to often form a distributed system
  o Increases the overall complexity of the resulting architecture over traditional real-time, embedded or services systems

• Cyber-physical systems include physical or virtual environments where people live, work and play that are instrumented and controlled by some form of computer system
Cyber-physical systems vs Internet of Things

- **Sensors**: gather information
- **Actuators**: initiate a physical action
- **Controllers**: monitor and adjust operating conditions of dynamical systems
- **Embedded Systems**: small computers with dedicated functions
- **Cyber-physical system**: computation, communications and physical processes depend on each other
- **Internet of Things**: computing paradigm where objects are intelligent and networked

CPS-Background: CPS and the 4th Industrial Revolution

“industry 4.0 is the trend towards automation and data exchange in manufacturing technologies and processes” [https://en.wikipedia.org/wiki/Industry_4.0](https://en.wikipedia.org/wiki/Industry_4.0)

CPS supposed to play a key role in Industry v4.0.

CPS enables smart applications and services to operate accurately and in real-time.

CPS and Industry v4.0 offer a significant economic potential: the German gross value will be boosted by a cumulative of 267 billion euros by 2025.

Cyber and physical systems are integrated: monitor, collect and exchange data and sensitive information in a real-time manner.
CPS can **sense the surrounding environment**, with the ability to **adapt and control the physical world**.

This is mainly attributed to their flexibility and capability to change the operation of system(s) process(es) through the use of real-time computing.
# CPS Layers

<table>
<thead>
<tr>
<th>Perception Layer:</th>
<th>Transmission Layer:</th>
<th>Application Layer:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensors</td>
<td>Cloud</td>
<td>Smart Waste Management</td>
</tr>
<tr>
<td>Aggregator</td>
<td>Internet</td>
<td>Smart Cars</td>
</tr>
<tr>
<td>Actuators</td>
<td>Access Point</td>
<td>Smart Transportation</td>
</tr>
<tr>
<td>RFID Tags</td>
<td>Wi-Fi</td>
<td>Smart Traffic Control</td>
</tr>
<tr>
<td>GPS</td>
<td>Routers</td>
<td>Smart Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Switches</td>
<td>Smart Street Lighting</td>
</tr>
<tr>
<td></td>
<td>ZigBee</td>
<td>Smart Water/Power Managements</td>
</tr>
</tbody>
</table>

**Layers:**

- **Perception Layer:**
  - Sensors
  - Aggregator
  - Actuators
  - RFID Tags
  - GPS

- **Transmission Layer:**
  - Cloud
  - Internet
  - Access Point
  - Wi-Fi
  - Routers
  - Switches
  - ZigBee

- **Application Layer:**
  - Smart Waste Management
  - Smart Cars
  - Smart Transportation
  - Smart Traffic Control
  - Smart Infrastructure
  - Smart Street Lighting
  - Smart Water/Power Managements

**Objective:**

- Data and Information Collection
- Data and Information Transmission
- Data and Information Analysis & Decision Making
1. CPS – Background
   - CPS Layers
   - CPS Use & Classification
   - CPS Components

2. CPS Security Alert
   - CPS Threats
   - CPS Vulnerabilities
   - CPS Attacks
   - CPS Challenges

3. CPS Security Measures
   - CPS Risk Management
   - Cryptographic Solutions
   - Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: Cyber Security and AI
## CPS Layers and Associated Attack Vectors

<table>
<thead>
<tr>
<th>Layers:</th>
<th>Objective:</th>
<th>Threat/Attack:</th>
<th>Target:</th>
<th>Security Measure:</th>
</tr>
</thead>
</table>
| **Perception Layer:** | Data and Information Collection | - Eavesdropping  
- Port Scan  
- Passive Replay | - Confidentiality  
- Privacy  
- Authentication | - Trust Management  
- Source Authentication  
- Secure Data/Systems  
- Data Protection |
| Sensors  
Aggregator  
Actuators  
RFID Tags  
GPS | | | | |
| **Transmission Layer:** | Data and Information Transmission | - Man-in-the-Middle  
- Meet-in-the-Middle  
- DoS/D-DoS  
- Repudiation  
- Replay | - Confidentiality  
- Integrity  
- Availability  
- Authentication | - Strong Password Policy  
- Strong Authentication  
- Lightweight Dynamic Symmetric Encryption  
- Secure Tunnelling |
| Cloud  
Internet  
Access Point  
WiFi  
Routers  
Switches  
ZigBee | | | | |
| **Application Layer:** | Data and Information Analysis & Decision Making | - Malicious Code Injection  
- Botnets - malware  
- Trojans  
- Worms  
- Buffer Overflow | - Privacy  
- Security  
- Safety  
- Authentication | - IDS/IPS  
- Firewalls  
- Strong Authentication  
- Strong Authorisation  
- Trust Management |
| Smart Waste Management  
Smart Cars  
Smart Transportation  
Smart Traffic Control  
Smart Infrastructure  
Smart Street Lighting  
Smart Water/Power Managements | | | | |
Cyber-physical attacks

- Cyber-physical attacks can be characterized by their impact in cyberspace and the corresponding impact in physical space.

Cyber-physical attacks

• **Breach of physical privacy**
  o Confidentiality of people’s real-time blood sugar level
  o The number of occupants in a house
  o Other private information collected from sensors

• **Unauthorized actuation**
  o Unauthorized user initiates actuation by breaching the integrity of a computer system that controls an actuator

• **Incorrect actuation**
  o The adversary aims to affect an actuator’s operation by breaching the integrity or availability of the instructions sent to it, the sensor data on which it relies, or its controller’s operation
  o Example: an attack that would consistently lower the speed values reported by a car’s sensors, so as to cause its cruise control system to keep accelerating.
Cyber-physical attacks

• **Delayed actuation**
  - The adversary delays actuation by breaching the integrity or availability of the data and systems involved. Suppression of warnings can also be included in this category.
  - Example: denial of service attack to delay measurements on dangerous pressures to be reported to a gas pipeline’s safety valve controllers.

• **Prevented actuation**
  - The adversary blocks actuation altogether by breaching the integrity or availability of the data and systems involved.
  - **EX-1**: Sleep deprivation attack that exhausts the battery of a surveillance robot or a medical implant until it can no longer function.
  - **EX-2**: Malware infection that suppresses the operation of a car window by injecting a “close” command every time an “open” command is received.
A cyber-physical attack is a security breach in cyberspace that adversely affects physical space.
1. CPS – Background
   - CPS Layers
   - CPS Use & Classification
   - CPS Components

2. CPS Security Alert
   - CPS Threats
   - CPS Vulnerabilities
   - CPS Attacks
   - CPS Challenges

3. CPS Security Measures
   - CPS Risk Management
   - Cryptographic Solutions
   - Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: Cyber Security and AI
CPS Risk Management
CPS Security Constraints and Challenges

There are constraints that limit secure operations, and solutions must take these constraints into consideration.

- **Authentication Challenges**
  - Weak Authentication Practices
  - Single/Two Factor Authentication
  - Lack of Biometric Use

- **Big Data Challenges**
  - Huge Data Amount
  - Lack of Real-Time Processing
  - Lack of Accountability
  - Lack of Real-Time Data Protection
  - Privacy Breaches
  - Trade-Off Issues

- **Access Control Challenges**
  - Single Sign On
  - Abuse of Privileges
  - Lack of Employee Screening
  - Access Control Issues

- **Supply Chains Challenges**
  - Real-Time Management Issues
  - Traffic Issues
  - Scheduling Issues
Research Goals

Security

Confidentiality

Data Confidentiality

Privacy

Integrity

Data Integrity

System Integrity

Availability

Data Availability

System Availability

Authentication

Source Authentication

Entity Authentication
The secret: is in how to generate secrets!
What is Cryptography (www.m-w.com)

cryptography noun

cryp·to·gra·phy | /ˈkrip-tä-grä-fē/

Definition of cryptography

1  : secret writing

2  : the enciphering and deciphering of messages in secret code or cipher
   also : the computerized encoding and decoding of information

3  : CRYPTANALYSIS
Security Solutions: A bit more Technical

**Security Solutions**

**Cryptographic approach**

- **Cryptographic Algorithms**
- **Cryptographic Protocols**

**Non-cryptographic approach**

- **Logical Protection:**
  - Intrusion Detection/Prevention System
  - Honeypot
  - Firewall
- **Physical Protection**
Cryptographic Solutions (mainly data protection)

Encrypt = lock
Decrypt = unlock

Key = password

Encryption = Algorithm + Key

Algorithm: Known to all
Key: Secret
Cryptographic Solutions (mainly data protection)

cipher: secret or disguised way of writing a code
Cryptographic Solutions (mainly data protection)
Cryptographic Solutions (mainly data protection)

Attackers Objectives:
1. Decrypt the message  
2. Recover Key  

Simpler  
Tougher
Cryptographic Solutions (mainly data protection)

Attackers Objectives:
1. Decrypt the message
2. Recover Key

- Advanced technologies: attackers can break more codes
- Therefore we need
  1. Complex yet efficient encryption algorithms and
  2. Key generation and management systems
• Typically, data confidentiality, data integrity, and data origin authentication are ensured by using symmetric cryptographic algorithms (require $r$ rounds).

• AES for example
  • 4 primitives per round
  • Multiple rounds

| $|K|$  | $r$ |
|------|-----|
| 128  | 10  |
| 196  | 12  |
| 256  | 14  |
Security Solutions

- Traditional solutions might have a **negative impact** on the CPS system performance:
  - Delay-sensitive and stringent QoS requirements
  - Devices with limited battery lifetime and limited computation

![Diagram of AES encryption process]

| | \(|K|\) | \(r\) |
|---|---|---|
| 128 | 10 |
| 196 | 12 |
| 256 | 14 |
Security Solutions

• **Solution**: New lightweight symmetric cryptographic algorithms and protocols that use dynamic key-dependent cipher structure

• Introduce savings
  • Round level
  • Number of Rounds

| | 
|---|---|
| | 
|\(|K|\) | | \(r\) | 
|128 | 10 |
|196 | 12 |
|256 | 14 |
Future Work: Non-Cryptographic Solutions

• Cryptographic solutions need to be complemented with non-cryptographic solutions

• The latter leverage AI to enable behavioral analysis of the network

• The research group is currently advancing the research in the following areas

1. IDS/IPS Systems, based on either
   o Signature
   o Specification
   o Anomaly detection
   o Security Information and Event Management (SIEM) systems

2. Honeypots and Deception techniques
IDS Classification

IDS Architecture (Source of data)
- Host-Based
- Network-Based
- Hybrid

IDS Reaction-Response
- Passive
- Active

IDS Detection Methods
- Signature detection or Misuses detection
- Anomaly detection
  - Self-learning
    - Time Series
    - Machine Learning
  - Programmed
    - Threshold
    - Simple rule based
    - Statistical model

IDS Locality
- Distributed
- Centralized
- Hybrid

Decision Methods
- Autonomous
- Cooperative

Specification protocol Analysis
Honeypot Classification
“a decoy system set up with deliberate weaknesses and a high profile to attract attacks for the purpose of analysis”
1. CPS – Background
   - CPS Layers
   - CPS Use & Classification
   - CPS Components

2. CPS Security Alert
   - CPS Threats
   - CPS Vulnerabilities
   - CPS Attacks
   - CPS Challenges

3. CPS Security Measures
   - CPS Risk Management
   - Cryptographic Solutions
   - Non-Cryptographic Solutions

4. Lessons Learnt

5. Trending: CyberSecurity and AI
Lessons learned

**Maintaining Security Services:** new lightweight cryptographic solutions to secure Cyber-Physical systems and IoCPT in real-time operations with minimum computational complexity.

**Confidentiality:** a new class of lightweight block or stream cipher algorithms to secure CPS resource-constrained real-time communications.

**Protecting Digital Evidences:** to overcome eliminating sources of evidence that trace back to the attack source, such as the case of Shamoon, Duqu, Flame and Stuxnet malware types.

**Enforcing Compliance:** respecting users' privacy by ensuring data access regulatory compliance, especially when stored by utility providers.
# Suggestions & Recommendations

## Prevention Layer

<table>
<thead>
<tr>
<th>Authentication Sub-layer</th>
<th>Prevention Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• User/Device Authentication:</td>
<td>• User/Device Authentication:</td>
</tr>
<tr>
<td>• Multi-factor Authentication</td>
<td>• Multi-factor Authentication</td>
</tr>
<tr>
<td>• Physical Protection</td>
<td>• Physical Protection</td>
</tr>
<tr>
<td>• Strong and Variable Password</td>
<td>• Strong and Variable Password</td>
</tr>
<tr>
<td>• Source Authentication and Message Integrity</td>
<td>• Source Authentication and Message Integrity</td>
</tr>
<tr>
<td>• Access Control</td>
<td>• Access Control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privacy Sub-layer</th>
<th>Prevention Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Patients Privacy</td>
<td>• Patients Privacy</td>
</tr>
<tr>
<td>• Anonymity (Pseudonymity)</td>
<td>• Anonymity (Pseudonymity)</td>
</tr>
<tr>
<td>• Proxies VPN</td>
<td>• Proxies VPN</td>
</tr>
<tr>
<td>• Preserving Privacy at Cloud (Differential Privacy, Secret Sharing, Homomorphic Encryption)</td>
<td>• Preserving Privacy at Cloud (Differential Privacy, Secret Sharing, Homomorphic Encryption)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Confidentiality Sub-layer</th>
<th>Prevention Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Encryption Algorithm</td>
<td>• Encryption Algorithm</td>
</tr>
</tbody>
</table>

## Defensive Layer

<table>
<thead>
<tr>
<th>Detection Sub-layer</th>
<th>Defensive Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Intrusion Detection Systems (Anti-malware)</td>
<td>• Intrusion Detection Systems (Anti-malware)</td>
</tr>
<tr>
<td>• SIEM</td>
<td>• SIEM</td>
</tr>
<tr>
<td>• Honeypots</td>
<td>• Honeypots</td>
</tr>
<tr>
<td>• Data System Integrity</td>
<td>• Data System Integrity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Correction Sub-layer</th>
<th>Defensive Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Intrusion Prevention Systems</td>
<td>• Intrusion Prevention Systems</td>
</tr>
<tr>
<td>• Firewalls</td>
<td>• Firewalls</td>
</tr>
<tr>
<td>• Data Backup</td>
<td>• Data Backup</td>
</tr>
<tr>
<td>• Alternative Devices and Configuration</td>
<td>• Alternative Devices and Configuration</td>
</tr>
</tbody>
</table>
Cybersecurity and AI

1. AI for Network Resilience
2. IoT Device Identification
3. Abnormal Traffic Detection
4. Guarding against Traffic Analysis
1. AI for Network Resilience: Motivation

- There is no security without verifying network consistency
Proposed Architecture

• **Solution**: we propose a Neural Network overlay on top of Software Defined Networks (SDN)

  Distributed Extraction + Distributed Processing + Centralized Management

• **Key Contributions**:
  - Edge Feature extraction
  - AI based overlay network over the data plane
  - Distributed processing over different nodes
  - Decision making at the data plane level
  - SDN Controller optimizes and monitors the distribution process
## SDN: Security Results

<table>
<thead>
<tr>
<th>Technique</th>
<th>Anomaly Detection (Balanced Data)</th>
<th>Anomaly Detection (Unbalanced Data)</th>
<th>Attack Identification (Balanced Data)</th>
<th>Attack Identification (Unbalanced Data)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Forest</td>
<td>99.2%</td>
<td>99.3%</td>
<td>98.3%</td>
<td>99.61%</td>
</tr>
<tr>
<td>SVM</td>
<td>96.74%</td>
<td>96.93%</td>
<td>90.64%</td>
<td>93.6%</td>
</tr>
<tr>
<td>KNN</td>
<td>94.5%</td>
<td>96.4%</td>
<td>90.19%</td>
<td>90.5%</td>
</tr>
<tr>
<td>DT</td>
<td>95.76%</td>
<td>96.4%</td>
<td>89.5%</td>
<td>90.89%</td>
</tr>
<tr>
<td>MLP</td>
<td>97.5%</td>
<td>97.0%</td>
<td>94.3%</td>
<td>92.73%</td>
</tr>
<tr>
<td>BPNN</td>
<td>98.7%</td>
<td>98.6%</td>
<td>77.2%</td>
<td>75.8%</td>
</tr>
<tr>
<td>DNN</td>
<td>96.11%</td>
<td>96.13%</td>
<td>95.03%</td>
<td>93.67%</td>
</tr>
</tbody>
</table>
### SDN: Consistency Results

<table>
<thead>
<tr>
<th>Technique</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConvNet</td>
<td>96%</td>
<td>96%</td>
<td>93%</td>
<td>90%</td>
</tr>
<tr>
<td>RNN</td>
<td>96%</td>
<td>83.4%</td>
<td>78.3%</td>
<td>78.5%</td>
</tr>
<tr>
<td>DNN</td>
<td>95.5%</td>
<td>93%</td>
<td>81.6%</td>
<td>77.5%</td>
</tr>
</tbody>
</table>
Flashback: CPS challenges

Security Constraints

- Hardware
  - Computational and energy constraint
  - Memory constraint
  - Tamper resistant packaging

- Software
  - Embedded software constraint
  - Dynamic security patch

- Network
  - Scalability
    - Diversity of devices
    - Diversity of communication medium
    - Multi-Protocol Networking
  - Dynamic network topology

With IoT and IoCPS: Rely on AI to classify malicious traffic for the variety of devices onboard
2. AI for IoT Traffic Classification (IoT Device Identification) Model—Accuracy

![Subsets of Features Accuracy Results with Random Forest](image-url)
AI for IoT Traffic Classification

Random Forest - Accuracy

<table>
<thead>
<tr>
<th>Model</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF</td>
<td>99.93%</td>
<td>0.999</td>
<td>0.999</td>
<td>0.9985</td>
</tr>
<tr>
<td>DT</td>
<td>99.85%</td>
<td>0.9977</td>
<td>0.9977</td>
<td>0.9977</td>
</tr>
<tr>
<td>RNN</td>
<td>99.77%</td>
<td>0.9965</td>
<td>0.9966</td>
<td>0.9965</td>
</tr>
<tr>
<td>ConvNet</td>
<td>99.78%</td>
<td>0.9971</td>
<td>0.9962</td>
<td>0.9966</td>
</tr>
<tr>
<td>ResNet</td>
<td>0.9978</td>
<td>0.997</td>
<td>0.9965</td>
<td>0.9967</td>
</tr>
</tbody>
</table>
3. AI for IoT Traffic Classification

Normal vs Attack Traffic - Accuracy

<table>
<thead>
<tr>
<th>Model</th>
<th>Accuracy</th>
<th>Precision</th>
<th>Recall</th>
<th>F1-score</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF</td>
<td>97.14%</td>
<td>0.8581</td>
<td>0.8628</td>
<td>0.8601</td>
</tr>
<tr>
<td>DT</td>
<td>96.28%</td>
<td>0.8299</td>
<td>0.8034</td>
<td>0.8157</td>
</tr>
<tr>
<td>RNN</td>
<td>95.35%</td>
<td>0.7925</td>
<td>0.9459</td>
<td>0.8469</td>
</tr>
<tr>
<td>ConvNet</td>
<td>95.16%</td>
<td>0.7872</td>
<td>0.9394</td>
<td>0.8410</td>
</tr>
<tr>
<td>ResNet</td>
<td>94.77%</td>
<td>0.7777</td>
<td>0.9533</td>
<td>0.8363</td>
</tr>
</tbody>
</table>
This covered few of the interesting topics the group is tackling
Selected Contributions

- New lightweight symmetric cryptographic algorithms and protocols that use dynamic key-dependent cipher structure
  - Achieving required cryptographic performance with reduced latency and resources
  - Efficiency, flexibility and robustness make the proposed solutions good candidates IoT systems

- Physical Unclonable functions and ID-based key distribution framework for smart grid security

- AI for reliability, modeling and statistical analysis of systems designs
Conclusions

- CPS part of 4th industrial revolution
- Privacy and Security key functional requirements
- Lightweight cryptography and non-cryptographic defensive/preventive measures are needed
- AI plays key role in cybersecurity of CPS
Thank You

You

Wish

a Secure Day