A PUF Based Approach for Sustainable Cybersecurity in Smart Agriculture

Presenter: Venkata K. V. V. Bathalapalli

Venkata K. V. V. Bathalapalli[1], S. P. Mohanty[2], E. Kougianos[3], Venkata P. Yanambaka[4],
Babu K. Baniya [5], Bibhudutta Rout[6]

University of North Texas, Denton, TX, USA.[1,2,3,6]

Central Michigan University, USA.[4]

Grambling State University, USA.[5]

Email: vb0194@unt.edu[1], saraju.mohanty@unt.edu[2], elias.kougianos@unt.edu[3],
yanam1.v@cmich.edu[4] , baniyab@gram.edu[5], , Bibhudutta.Rout@unt.edu[6]

Outline of the talk

- □ Introduction
- □ Applications of IoT
- □ Internet of Agro-Things
- □ Novel Contributions
- □ PUF Based Hardware-Assisted Security for IoAT
- □ Implementation and Validation
- □ Conclusion and Future Research

Applications of Internet of Things (IoT)

Smart Farming

Smart City

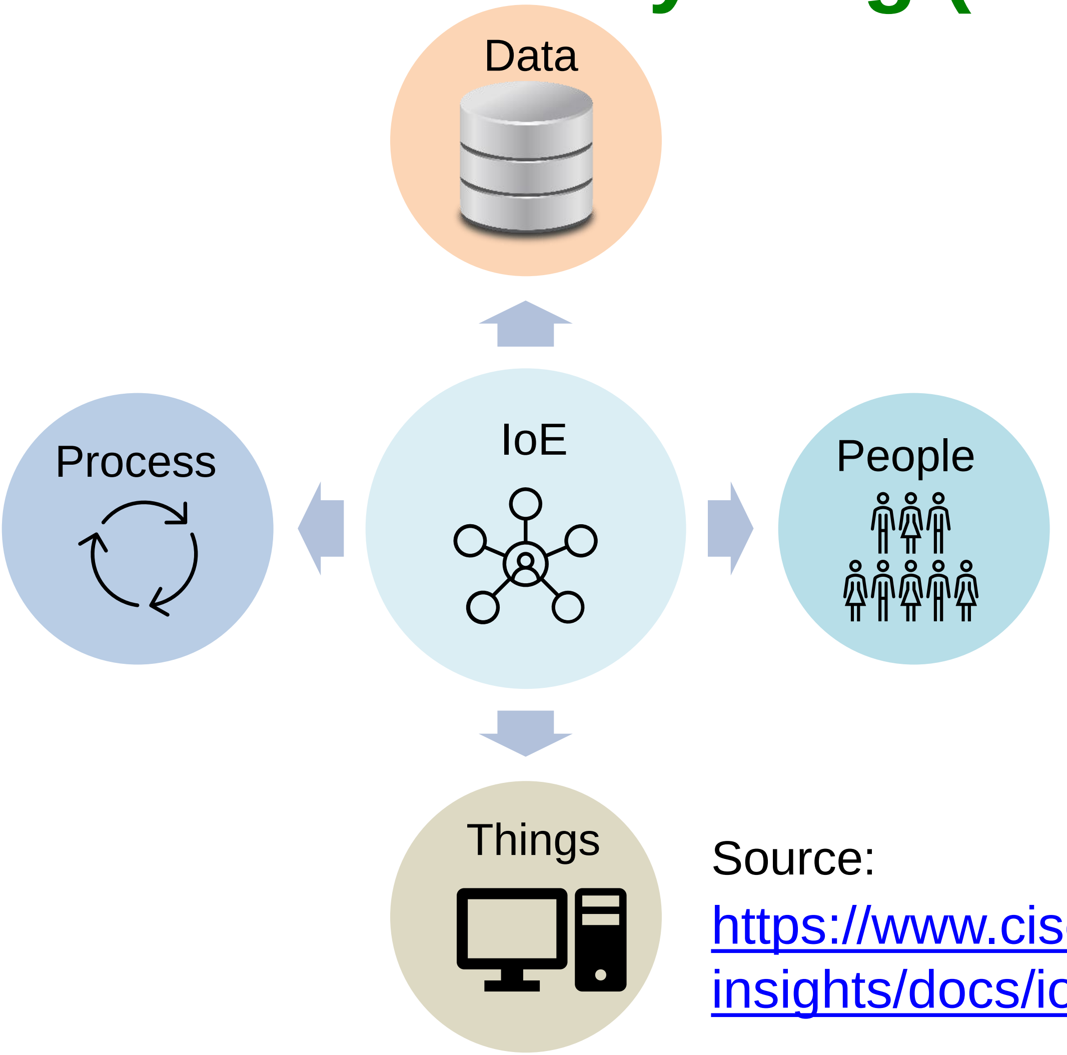
Smart Health

Smart Grid

Smart Home

Smart Transportation

Internet of Everything (IoE)



IoE: Internet of Everything is defined as a consolidated network of People, Process, Data and Things for Sustainable Smart City, Smart Healthcare, Smart Agriculture and Smart Transportation.

Source: https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf

IT Security vs IoT Security

Information Technology Security

- IT requires more computational resources for security solutions
- Limited varieties of IT devices
- IT security breach can be costly
- Information Technology infrastructure is constrained to a building

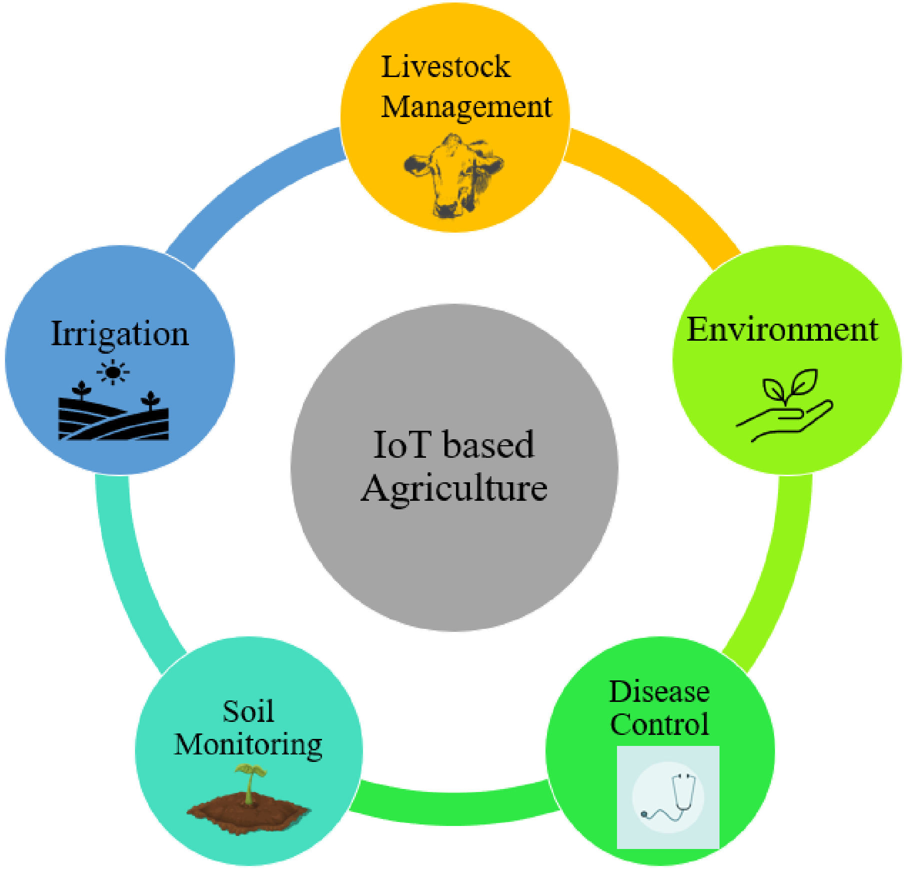
Source: S. P. Mohanty, Keynote Address, Secure IoT by Design, 4th IFIP International Internet of Things Conference (IFIP-IoT), 2021, Amsterdam, Netherlands, 5th November 2021

Internet of Things Security

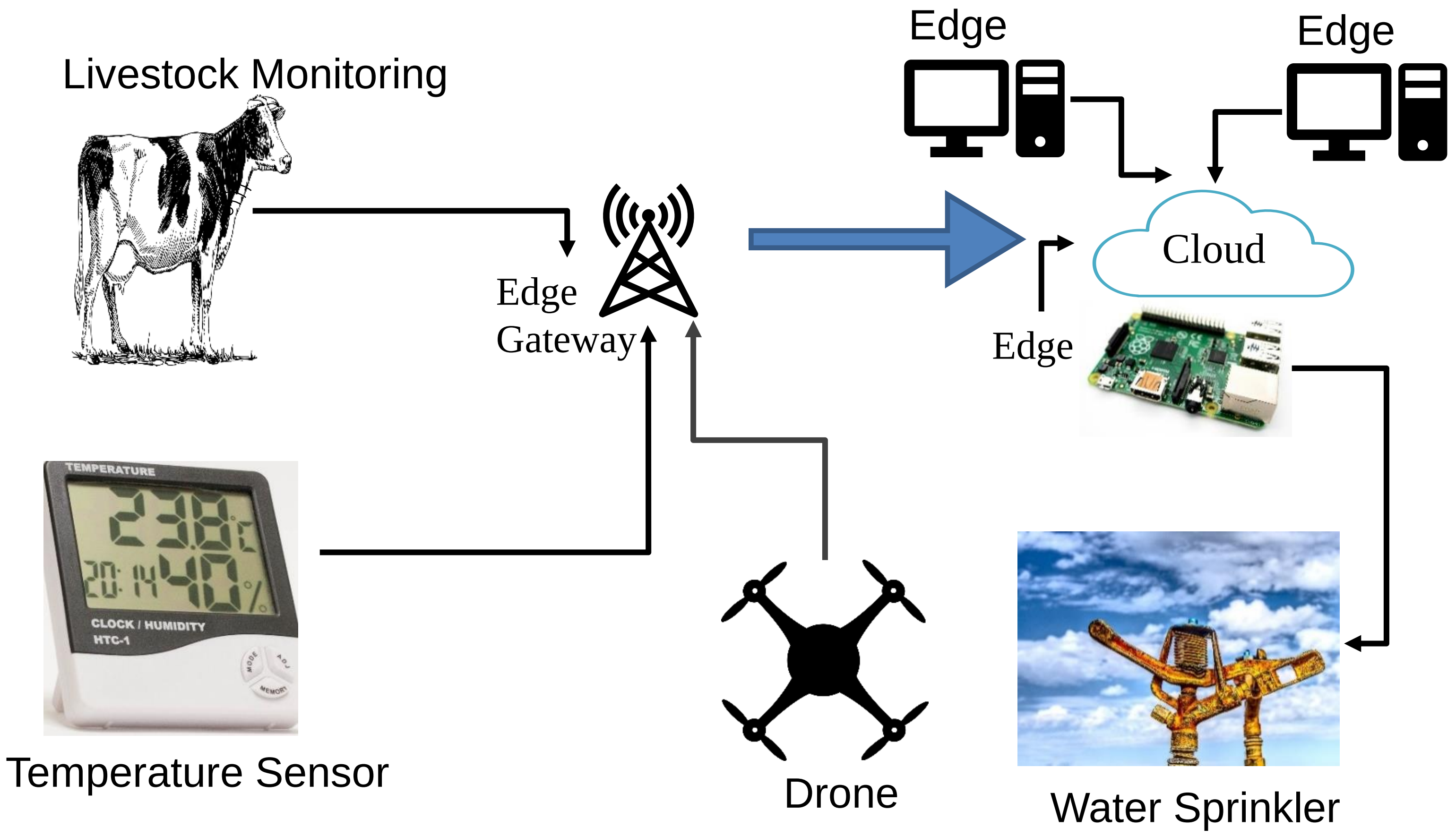
- IoT may not have computational resources to address security issues
- Large varieties of IoT devices(IoMT, IoAT)
- IoT security breach can be catastrophic and life threatening
- IoT infrastructure is deployed in open environment (Smart Village, Smart City)

Maintenance of security systems for Consumer electronics requires Energy and affects the overall performance.

Applications of IoT in Farming



Broadview of Internet of Agro-Things



Security Issues in IoAT

❑ Smart Farms are Hackable Farms: IoT in Agriculture can improve the efficiency in productivity and feed 8.5 billion people by 2030. But it can also become vulnerable to various cyber security threats.

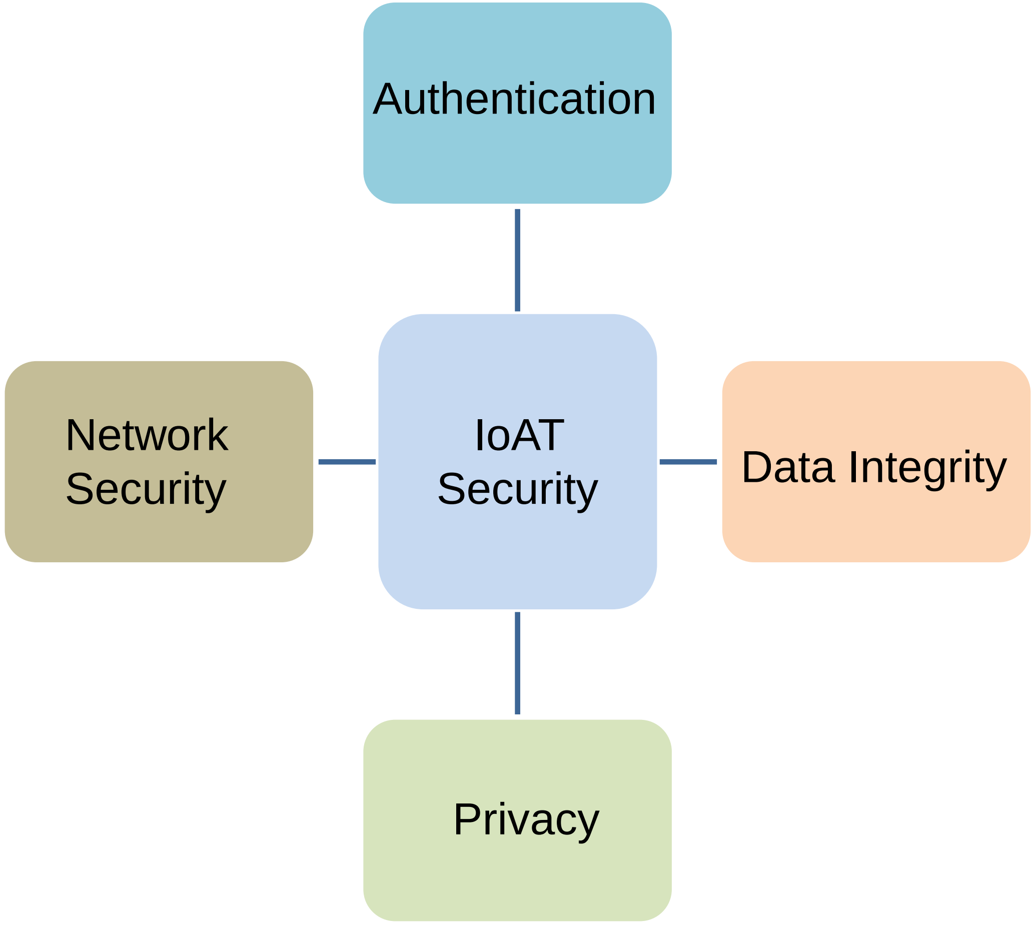
https://spectrum.ieee.org/cybersecurity-report-how-smart-farming-can-be-hacked

https://cacm.acm.org/news/251235-cybersecurity-report-smart-farms-are-hackable-farms/fulltext

❑ DHS report highlights that implementation of advanced precision farming technology in livestock monitoring and crop management sectors is also bringing new security issues along with efficiency

https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

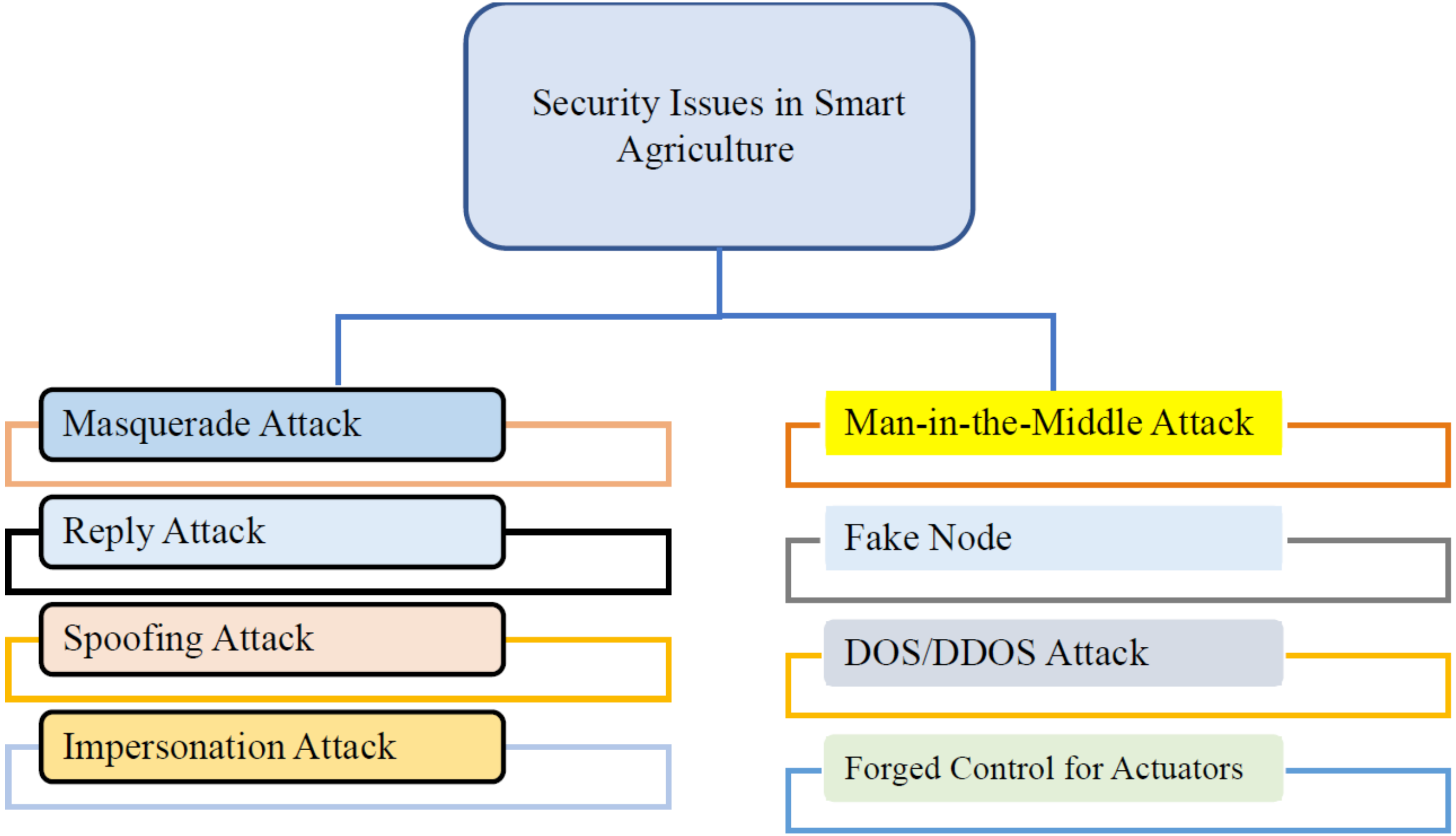
Security Requirements for IoAT



Internet of Agro-Things Characteristics:

- ✓ Smaller Size
- ✓ Smaller weight
- ✓ Safer Device
- ✓ Less Computational resources

Security Attacks on IoAT Devices



- Masquerade Attack: Obtaining unauthorized access to resources using false identity.
- Fake Node: Replacing the original sensor with malicious one.
- Reply Attack: A cyber criminal intercepting the communication between two devices and delaying or resending the message to disrupt the working of the system.

Related Research on Security in Smart Farming

Works	Objective	Features
Gupta, et al.[2020]	This research discusses major security vulnerabilities in Smart Agriculture and importance of data security in Smart Farming	Defines Precision Farming and security practices
Abuan, et al.[2014]	This research discusses the Implementation of Machine learning techniques for videos during Farm surveillance	Real time analysis and decision making
Barreto, et al. [2018]	This research Outlines security issues and challenges in Smart Agriculture	Highlights the security issues and challenges including agro-terrorism, ransomware and other cyber threats

Novel Contributions

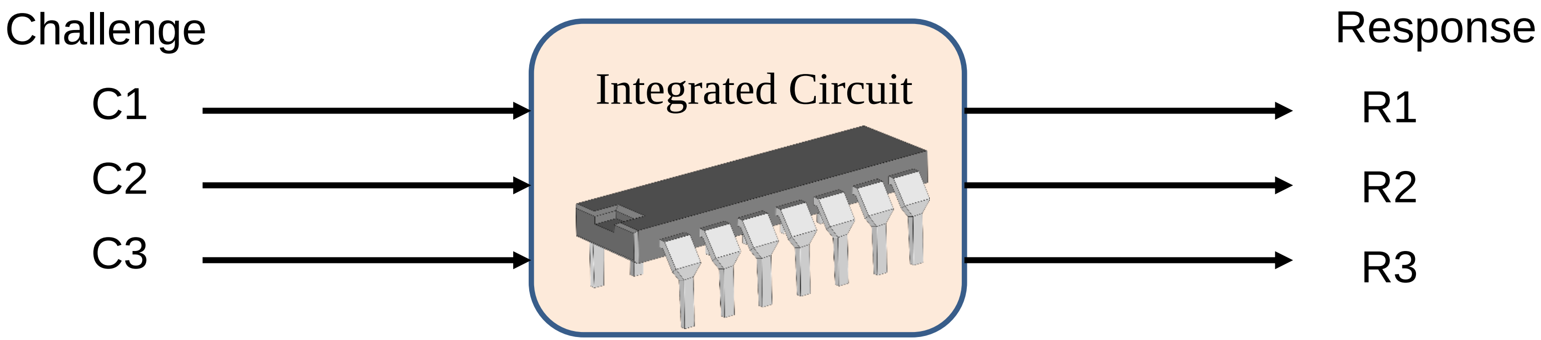
- A Hardware assisted security mechanism that utilizes hardware internal micro-manufacturing characteristics to design a robust hardware fingerprint (PUF key).
- A system that is driven by Edge Computing for swift processing, analysis and decision making.
- Strong, reliable and secure Arbiter PUF module with excellent randomness and uniqueness for robust and secure cryptographic key.
- A Simple and time efficient device authentication mechanism for Edge Computing driven smart farming applications.

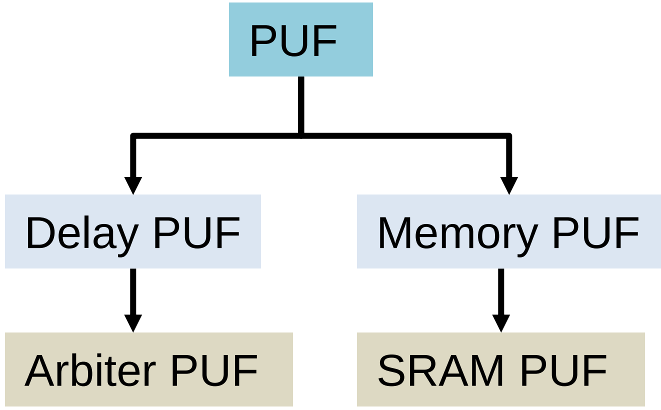
Physically Unclonable Functions (PUF)

- A Physically Unclonable Function is designed using hardware internal manufacturing variations.
- PUF module is simple to develop but highly impossible to duplicate.
- PUF module is considered as either strong or weak depending on the number of Challenge- Response Pairs(CRP).
- If a PUF supports large number of Challenge Response pairs, then it is considered as Strong PUF.
- PUF keys can be used as an Electronic Device fingerprints.

Working of PUF

- Input to a PUF is called as Challenge and Output from a PUF is called Response.

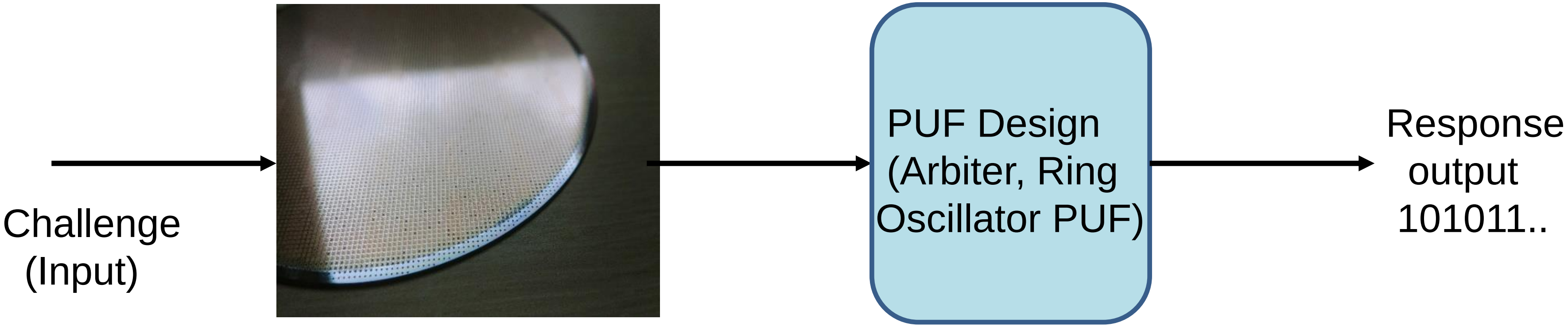




- A PUF generating large number of CRP is a strong PUF and PUF supporting small number of CRP is considered as Weak PUF.
- A PUF can be categorized as Delay and Memory based PUF. Delay PUF is based on the variations in wiring and variations at gates in silicon. Memory based PUF is based on the instability in the startup phase of SRAM cell.

PUF-Principle

- PUF keys are not stored in the digital memory. But the keys are generated using silicon manufacturing process variations.



Challenge (Input)

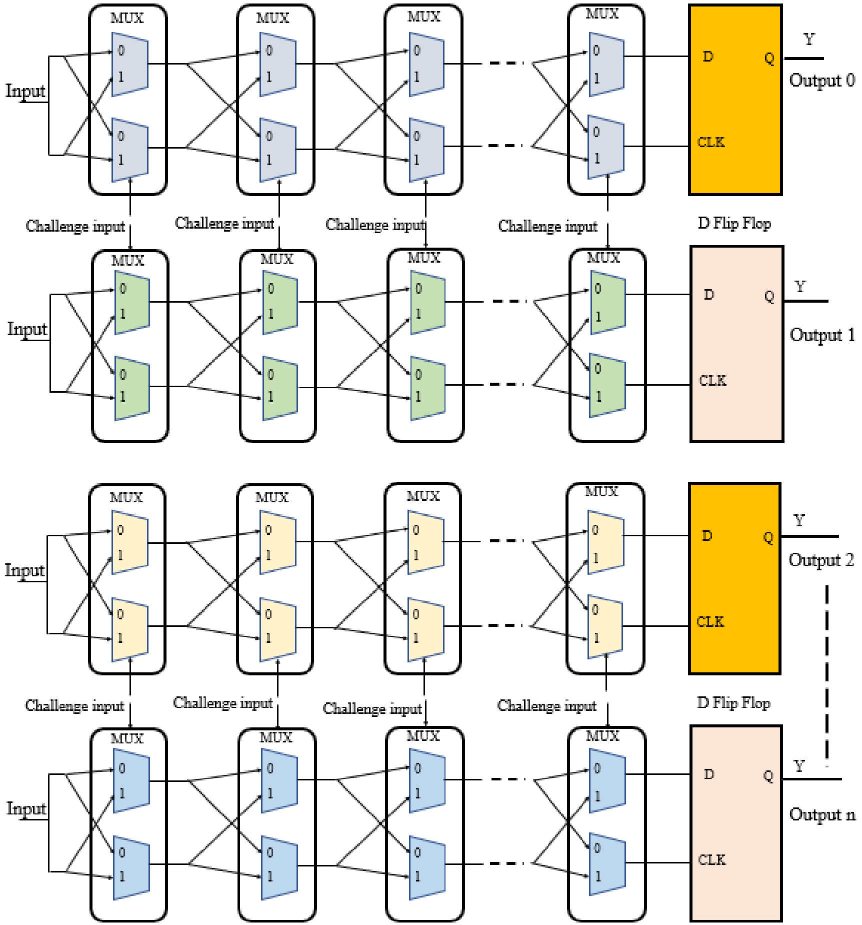
PUF Design (Arbiter, Ring Oscillator PUF)

Response output 101011..

Silicon Wafer

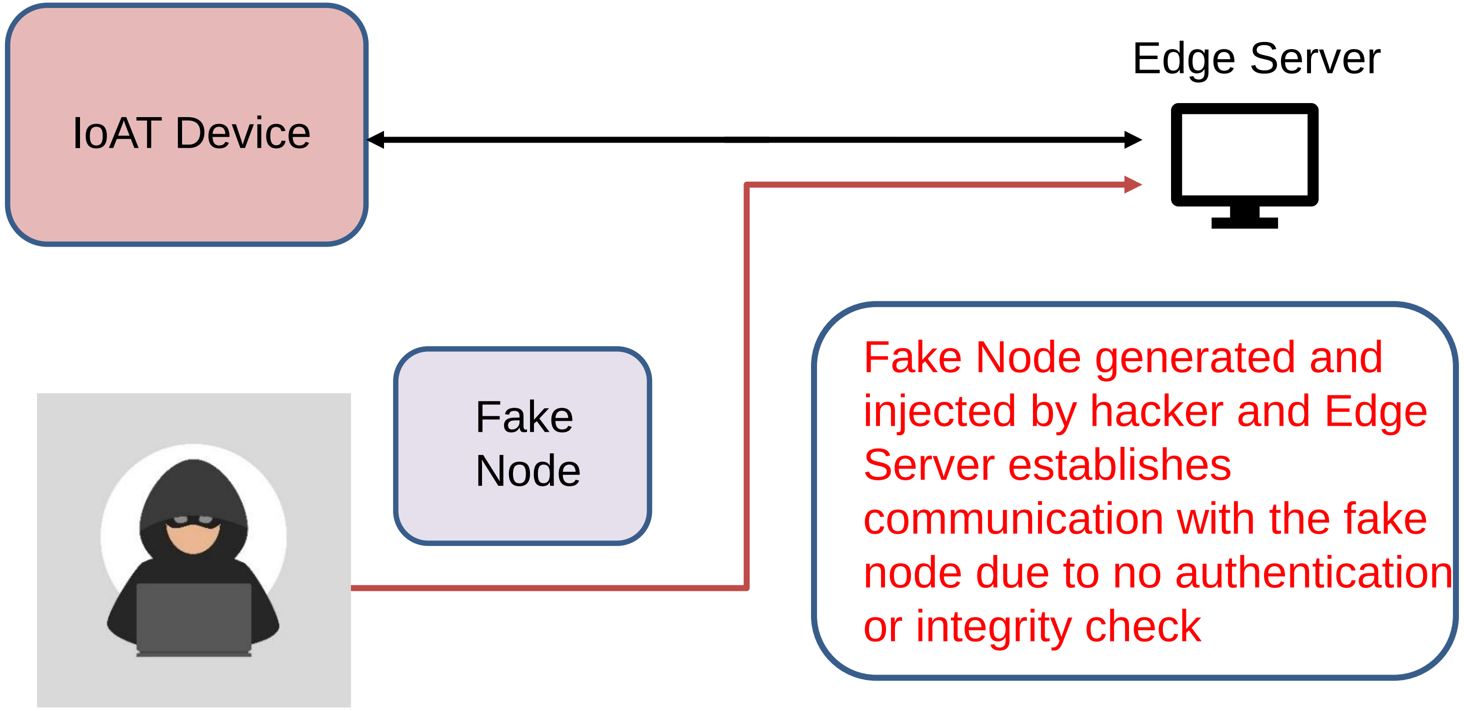
Parameters: Oxide growth, Ion Implantation, Lithography

Arbiter PUF



Strong PUF module which can be used for cryptographic purposes due to large number of CRP’s

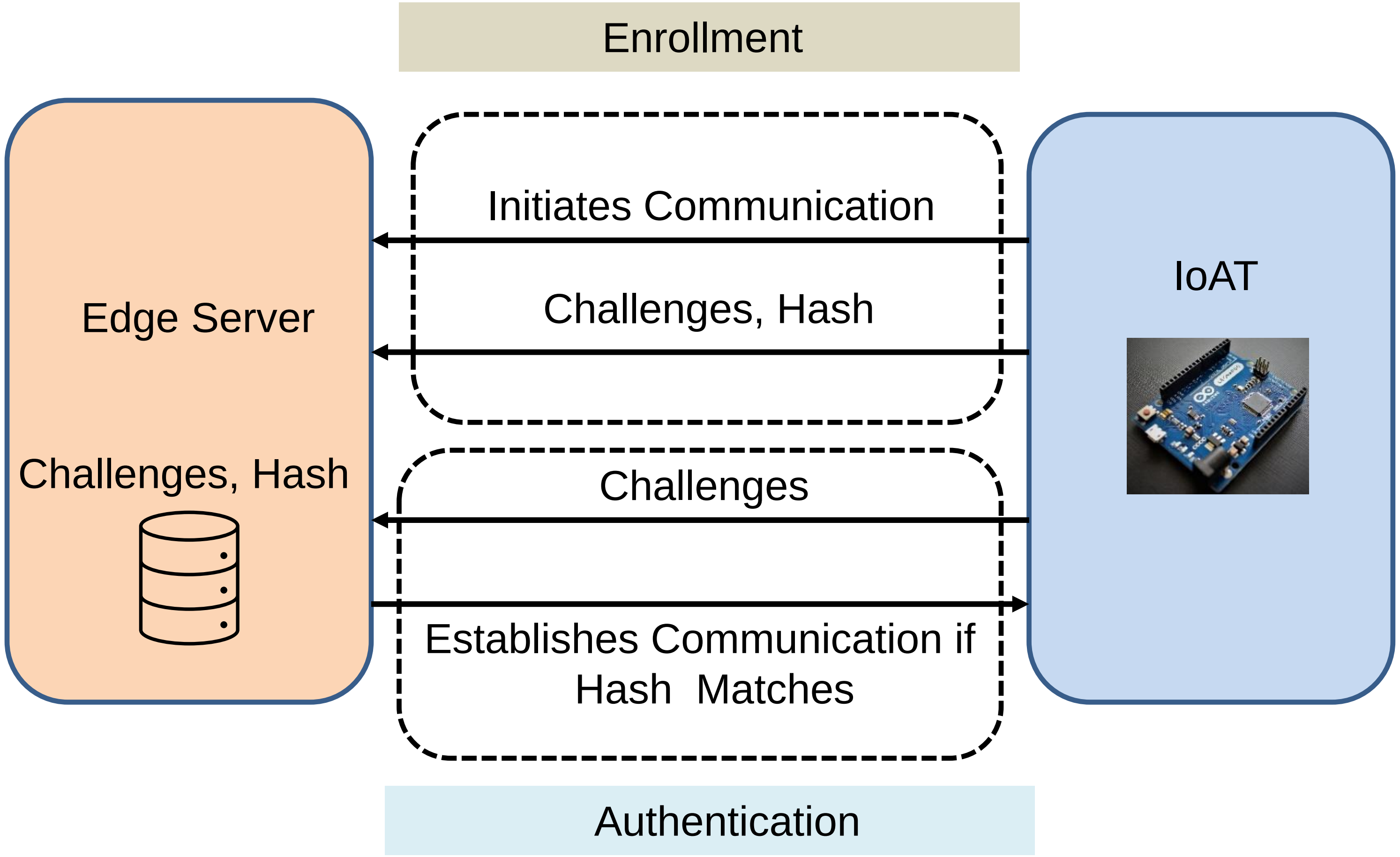
Threat Model



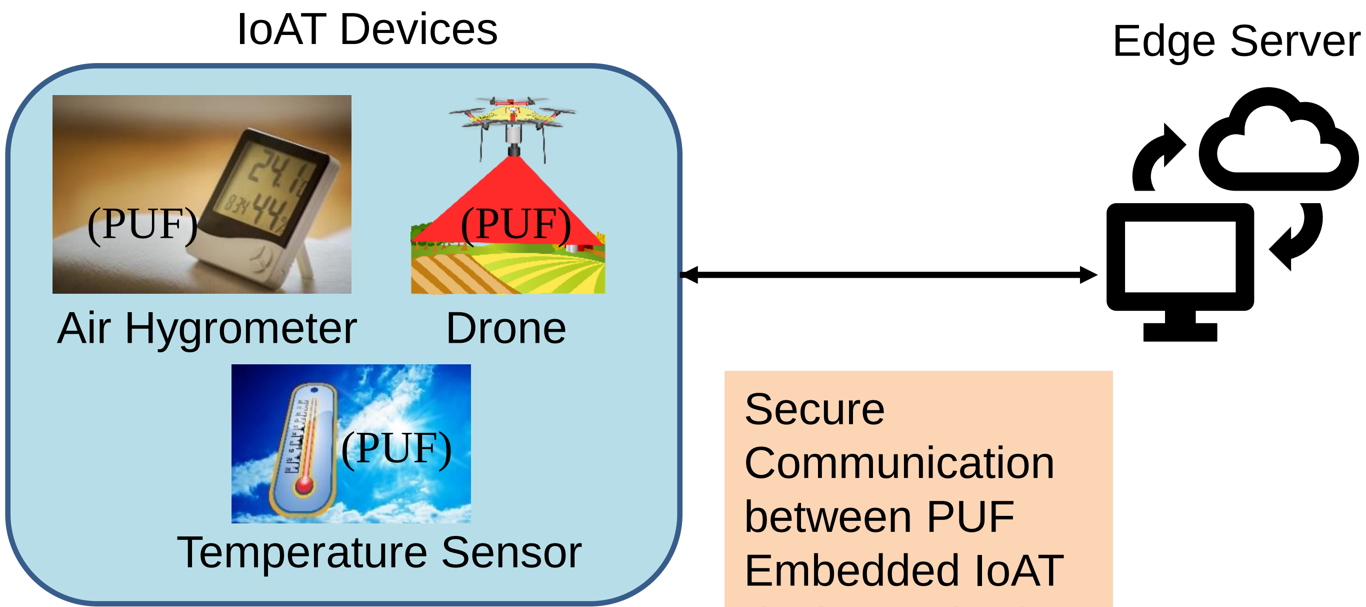
Fake Node generated and injected by hacker and Edge Server establishes communication with the fake node due to no authentication or integrity check

Malicious Node Generation and replacement

Authentication Process for IoAT



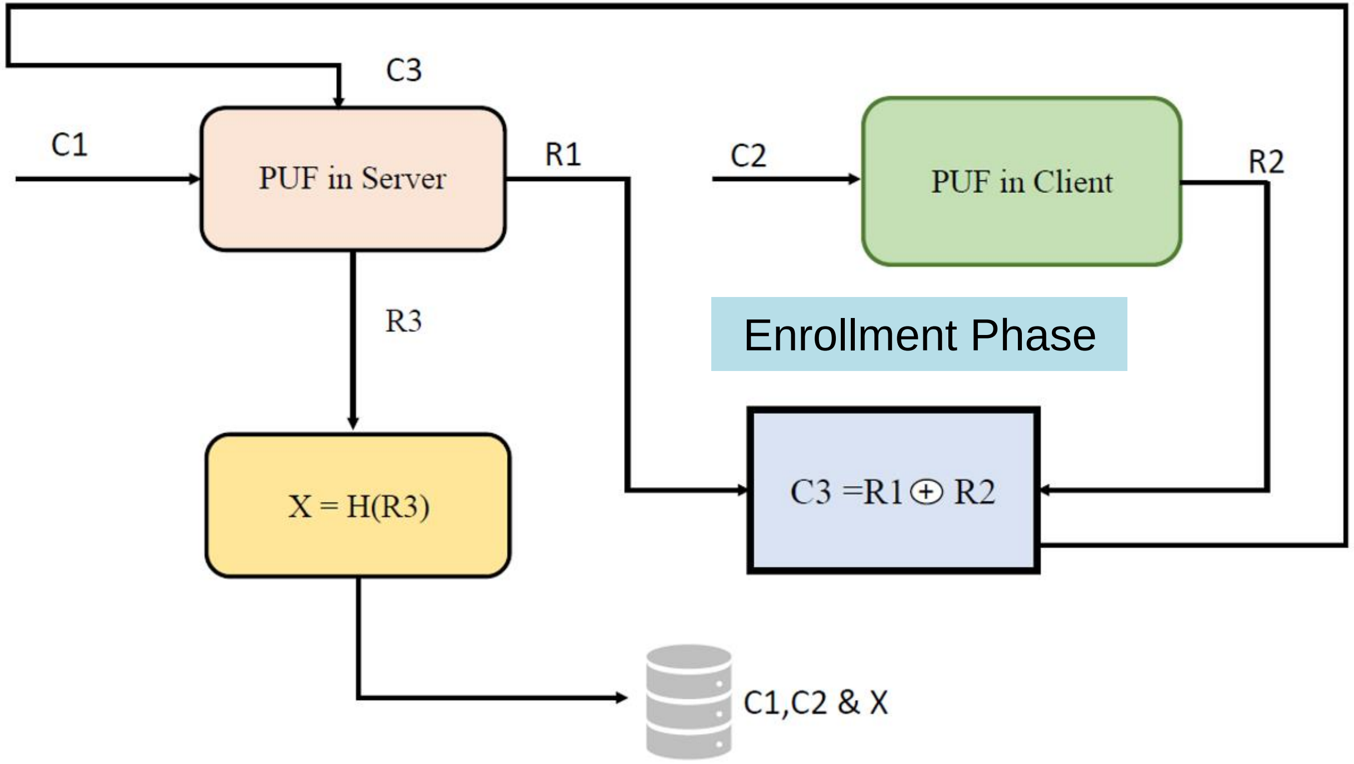
Secure Design Approach for Robust Internet of Agro-Things



Secure Communication between PUF Embedded IoAT device and Edge Server

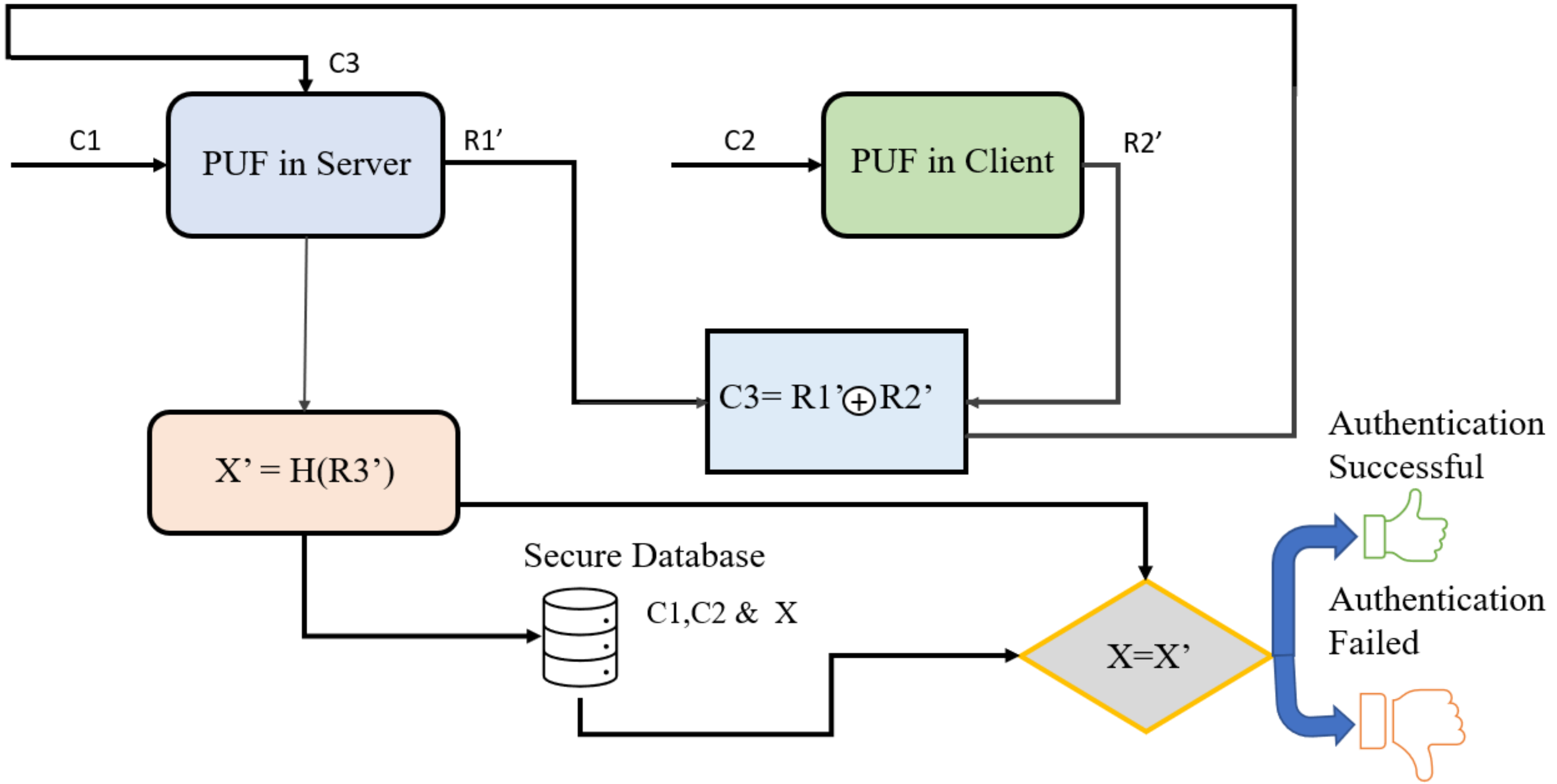
Edge Server authenticates the devices using the PUF key of each electronic device which is the fingerprint for that device

Enrollment Phase of the Proposed Security Protocol



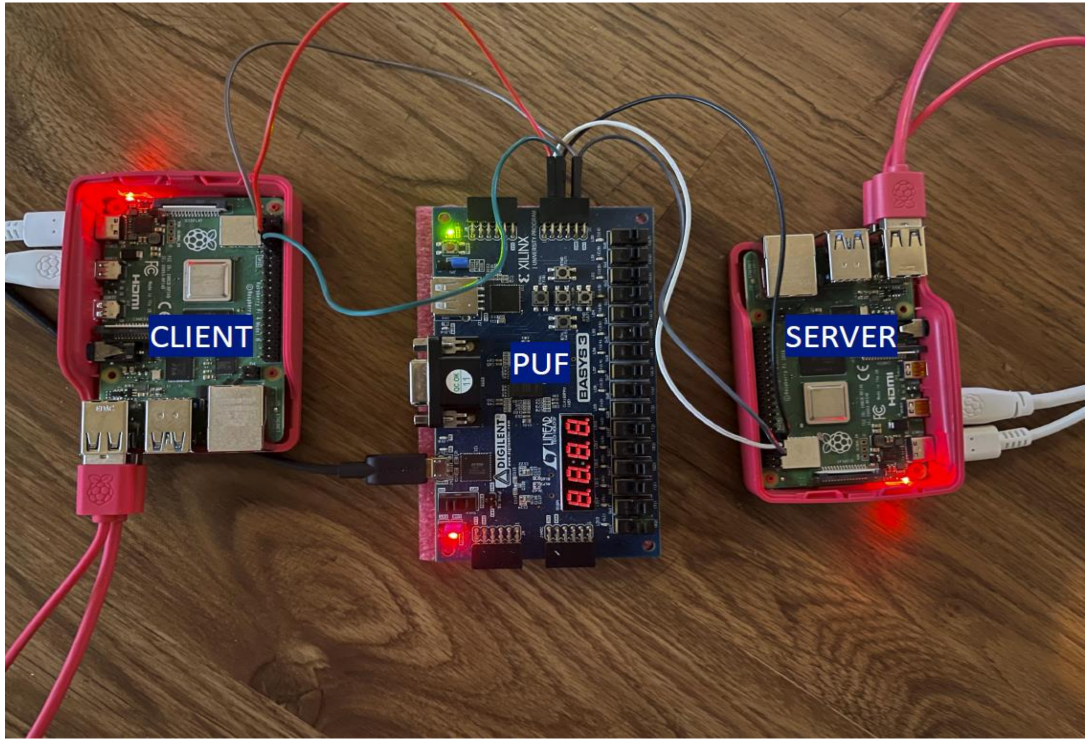
C1 => R1
C2 => R2
C3 = R1 XOR R2
C3 => R3
X = H(R3)
X, C1,C2 are stored in Database

Authentication Phase



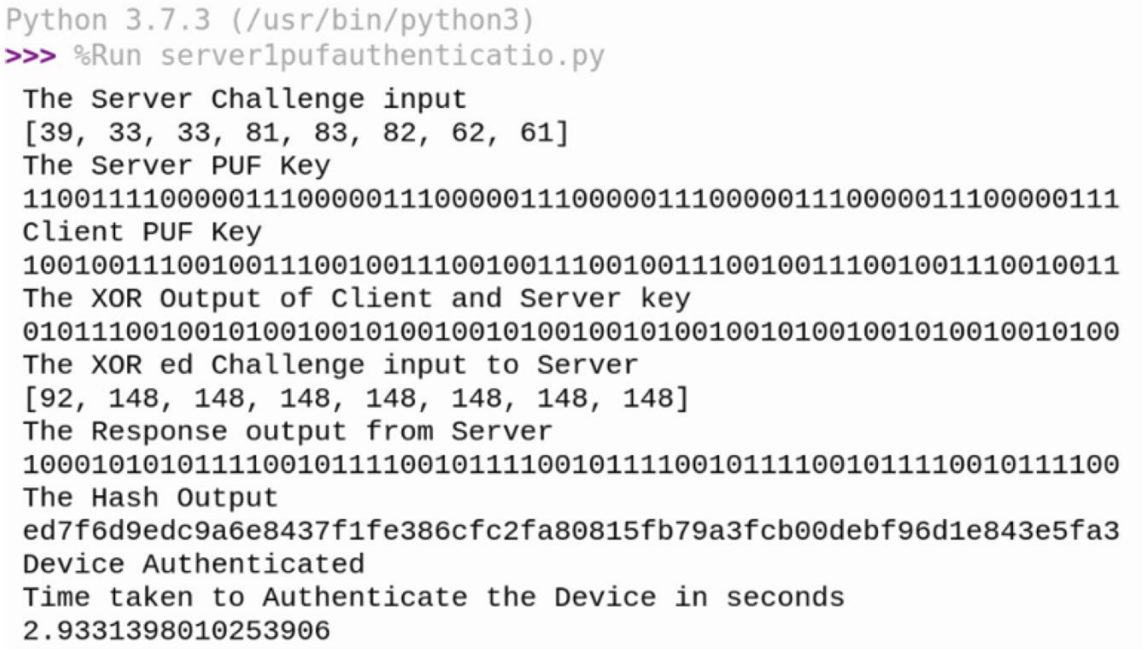
Only C1 and C2 are retrieved and given as inputs to the PUF module. The final Hash value X is compared with the stored hash value X to authenticate the device

Prototype of the Proposed Security Scheme



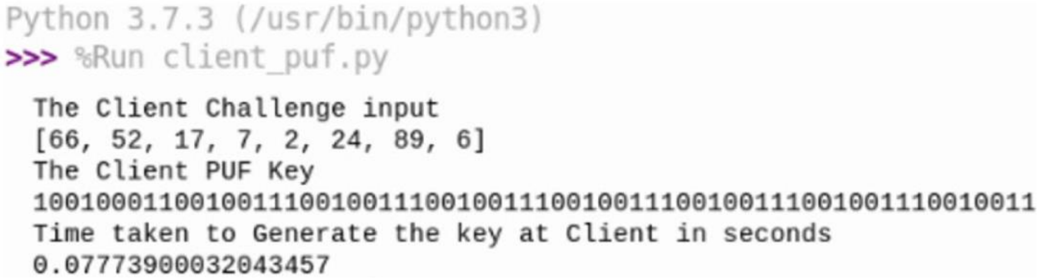
Parameter	Value
Hamming Distance	48%
Randomness	41.07%
Time Taken to Authenticate the Device in Seconds	0.16 to 2.93 Seconds
FPGA	Basys 3, Artix-7

Experimental Results



```
Python 3.7.3 (/usr/bin/python3)
>>> %Run server1pufauthenticatio.py
 The Server Challenge input
 [39, 33, 33, 81, 83, 82, 62, 61]
 The Server PUF Key
 1100111100000111000001110000011100000111000001110000011100000111
 Client PUF Key
 1001001110010011100100111001001110010011100100111001001110010011
 The XOR Output of Client and Server key
 0101110010010100100101001001010010010100100101001001010010010100
 The XOR ed Challenge input to Server
 [92, 148, 148, 148, 148, 148, 148, 148]
 The Response output from Server
 1000101010111100101111001011110010111100101111001011110010111100
 The Hash Output
 ed7f6d9edc9a6e8437f1fe386cfc2fa80815fb79a3fcb00debf96d1e843e5fa3
 Device Authenticated
 Time taken to Authenticate the Device in seconds
 2.9331398010253906
```

Server Output



```
Python 3.7.3 (/usr/bin/python3)
>>> %Run client_puf.py
  The Client Challenge input
  [66, 52, 17, 7, 2, 24, 89, 6]
  The Client PUF Key
  1001000110010011100100111001001110010011100100111001001110010011
  Time taken to Generate the key at Client in seconds
  0.07773900032043457
```

Client Output

Conclusion

- Cybersecurity issues in IoT based applications have now become the focal point for the research community.
- As IoT devices utilization is extending to Agriculture, security vulnerabilities of IoT devices are becoming bottlenecks for Smart Farming practices.
- Hardware and software assisted security solutions are possible for IoT assisted applications.
- This Paper focuses on Hardware Assisted security approach for Smart Farming where End IoT devices are equipped with PUF module thereby ensuring the authenticity of IoAT devices.

Direction for Future Research

Our future research interests include:

❑ Privacy and/ or Security by Design(PbD or SbD).

❑ Security, Privacy, IP Protection of Information and System (in Cyber-Physical Systems or CPS).

❑ Security of systems(e.g., Smart Healthcare device/data, Smart Grid, UAV, Smart Cars).

❑ Sustainable Smart City needs sustainable IoT/CPS

❑ Including device and data security into one model for Internet of Sustainable things.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant number HBCU-EiR-2101181.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s)
and do not necessarily reflect the views of the National Science Foundation.

Thank You !!!