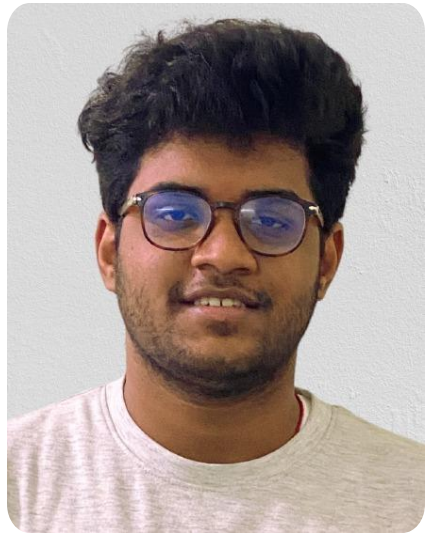
Preserving Privacy in Secure DNS in the context of IoT

- Team name – WPOP (We Protect Our Privacy)
- We are students from **International Institute of Information Technology Bangalore** (IIITB).
- **Dr. Jyostna Bapat**, Ph.D. (Pennsylvania State University), who works as a Professor at IIITB, is mentoring our team for this competition.
- We are a diverse team with specializations in Artificial Intelligence, Machine Learning, Networking Communication, and Cybersecurity.
- The areas of expertise of our mentor include wireless communication systems, cognitive radios, and communication for the Internet of Things.

Bharath Joshi

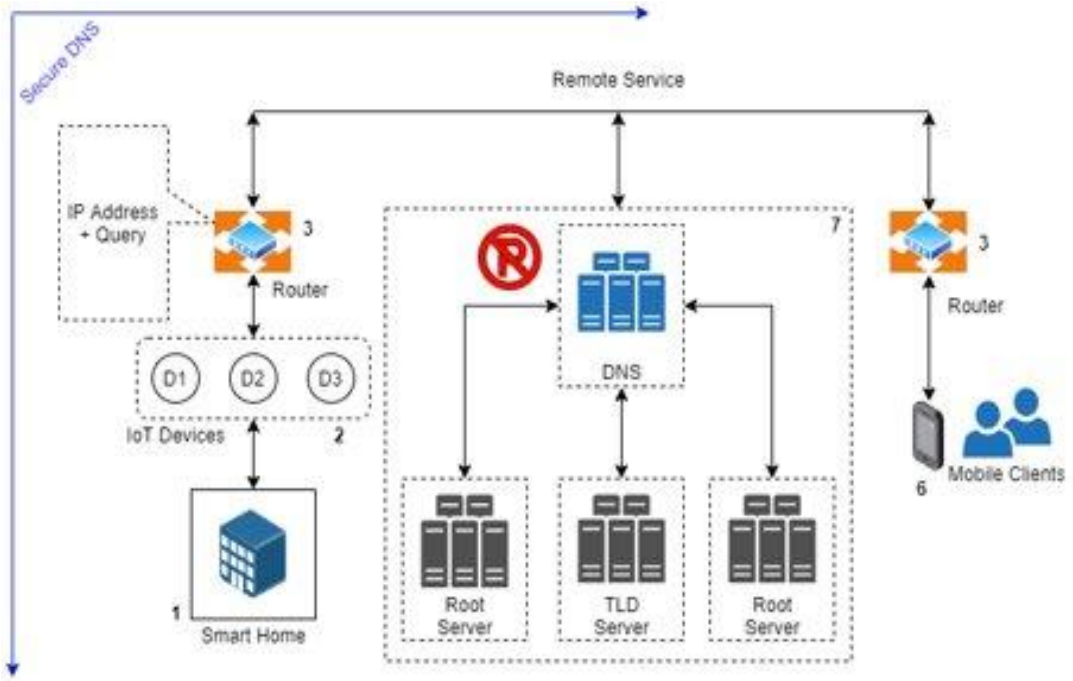
Krishna Phalgun (Captain)



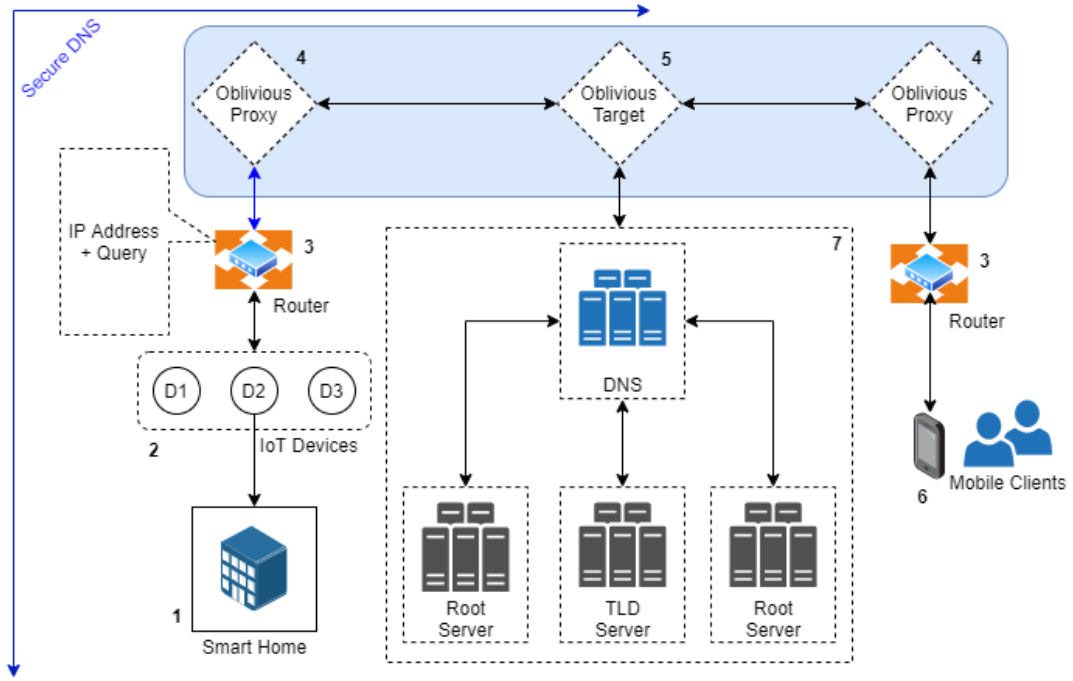
Sai Rithwik

Why is privacy in DNS important?

- Because everything we do on the internet begins with a query to the DNS.
- If one can see our queries in real time, one could create a detailed profile of ourselves, our interests, and our activities.
- Many actors appear to be using the DNS to monitor what we do online and censor which services we can access.
- As the Internet of Things (IoT) gets more widely adopted, privacy issues are becoming more prevalent, preventing greater adoption.



A schematic of the functioning of secure DNS highlights privacy concerns at the DNS operator.



A schematic showing how oblivious secure DNS works, which could help to solve privacy concerns.

What is the scope of the project?

The following questions will be answered as best as possible

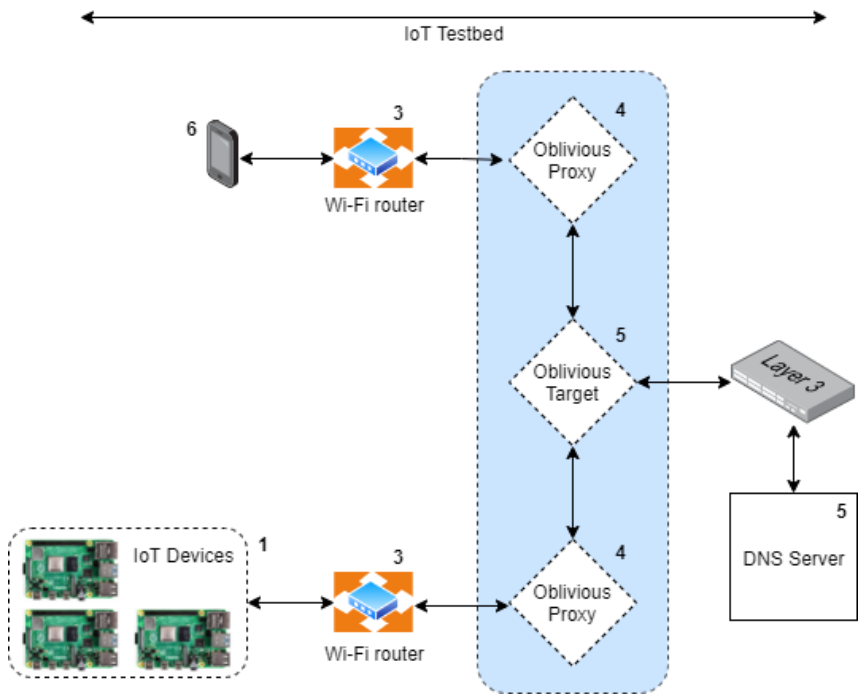
- Can eliminate unauthorized DNS surveillance?
- Can we make it more difficult to acquire individual activity profiles?
- What would it take to make ODoH feasible in the context of IoT?
- How to deal with common challenges in the context of the IoT while maintaining privacy?

According to mentors, this might serve as the basis for secure DNS implementation in IoT environments.

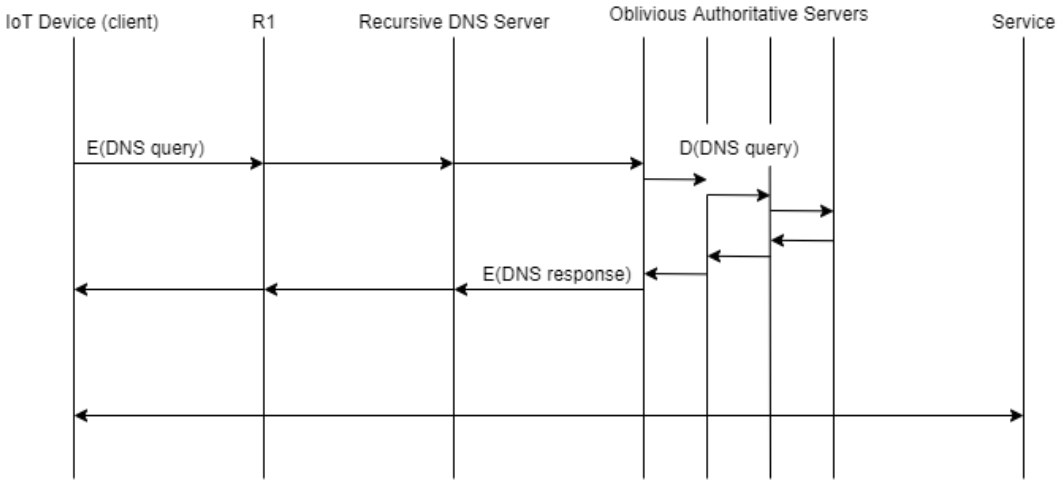
How do we implement the project?

This project, as mentors pointed out, has three components: integration, development, and qualitative analytics.

- The internal workings of the DNS will be investigated.
- To encrypt the DNS queries and responses, several asymmetric encryption methods will be studied.
- A testbed will be made, deployed, and evaluated for scalability, privacy enhancement, and performance.
- As suggested by mentors, existing proxy and target implementations will be reviewed and implemented in the context of the IoT.



A schematic of a possible testbed incorporating an oblivious solution for secure DNS.



A schematic of the event flow in the secure DNS following the incorporation of the oblivious solution.

Acknowledgements and References

This project would not have been possible without the support of many people. We are grateful to mentor Jyotsna Bapat, co-mentor Sasirekha GVK, and Pankaj Diwan, as well as mentors from NASSCOM CoE – IoT & AI and ICANN, for their invaluable support, comments, and encouragement.

1. https://odns.cs.princeton.edu/pdf/pets.pdf
2. https://ieeexplore.ieee.org/document/8651860
3. https://ieeexplore.ieee.org/document/8798622
4. https://ieeexplore.ieee.org/document/8653281
5. https://ieeexplore.ieee.org/document/9151339
6. https://www.slideshare.net/apnic/dns-privacy-133471512
7. https://team.inria.fr/privatics/files/2021/02/Thesis_PIVOT_Privatics_2020.pdf