

**PRIVACY-AWARE CACHING  
IN INFORMATION-CENTRIC  
NETWORKING**

**MICANS INFOTECH**



# ABSTRACT

- Information-Centric Networking (ICN) is an emerging networking paradigm where named and routable data (content) is the focal point.
- Users send explicit requests (interests) which specify content by name, and the network handles routing these interests to some entity capable of satisfying them with the appropriate data response (producer).
- One key feature of ICN is opportunistic in-network content caching.



- This property facilitates efficient content distribution by reducing bandwidth consumption, lessening network congestion, and improving the content retrieval latency by users (consumers).
- Unfortunately, the same feature is also detrimental to privacy of content consumers and producers. Simple to implement, and difficult to detect, timing attacks can exploit ICN routers as “oracles” and allow an adversary to learn whether a nearby consumer recently requested certain content.
- The attack leverages a timing side channel that relies on router caches and is implemented by requesting a few packets from each piece of content being probed.



# EXISTING SYSTEM

- Information-Centric Networking (ICN) is an emerging network architecture in which the focal point is named and routable data (content), rather than hosts and addresses.
- In ICN, a consumer requests content by name (i.e., expresses interests for the content) and the network takes care of finding and returning the data.
- The ICN approach moves hosts into the background by treating named content as a first-class object. One important ICN feature is opportunistic in-network content caching. Its goal is to reduce congestion while improving throughput and latency for popular content.



## DISADVANTAGES

- Encryption is not sufficient to mitigate these attacks.

MICANS INFOTECH



# PROPOSED SYSTEM

- Elaboration upon the efficacy of cache timing attacks in CCN and NDN – two types of ICN architectures.
- Extension of the cache privacy attack to local and distributed adversaries.
- Complete proofs for the privacy-preserving cache mechanisms.
- A protocol to improve the efficiency of privacy-preserving caches in trusted domains.

MICANS INFOTECH



## ADVANTAGES

- Its goal is to reduce congestion while improving throughput and latency for popular content

MICANS INFOTECH



# HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

MICANS INFOTECH





# SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

MICANS INFOTECH



# CONCLUSION

- This paper explored cache privacy in ICN (and CCN) and identified several important privacy threats. We then introduced some plausible and effective counter-measures.
- First, we suggest that consumers and producers should indicate which content is privacy-sensitive. Then, we proposed several techniques that provide certain tradeoffs between privacy and latency.
- These techniques were assessed with respect to local and distributed adversaries.



- We also introduced a formal model that allows us to quantify the degree of privacy offered by various caching algorithms.
- We believe that proposed techniques are general and may be of interest beyond caching. Items of future work include analyzing the depth of edge routers which must introduce content-specific artificial delays as well as techniques for consumers and producers to link distinct private content together to prevent correlation attacks

