Hierarchical Architecture for Mobile Object Authentication in the Context of IoT Smart Cities

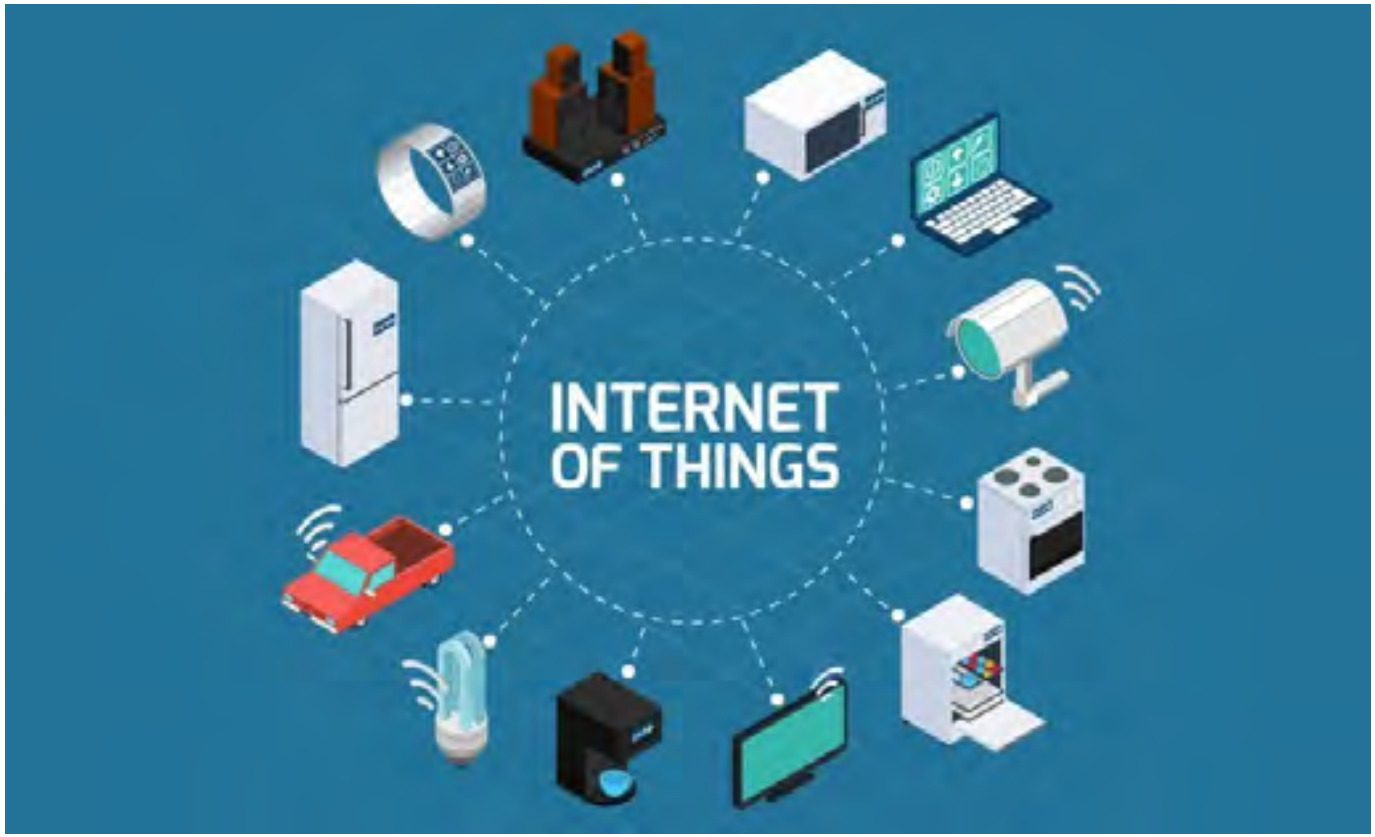
Maha Saadeh Azzam Sleit Khair Eddin Sabri
Wesam Almobaideen

The paper is published in the Journal of Network and Computer Applications, 2018, 121(1), 1–19.

Department of Computer Science, The University of Jordan
Amman, Jordan

Internet of Things (IoT)

- The Internet of Things (IoT) describe a network of physical objects that are connected and are used to collect and share data.

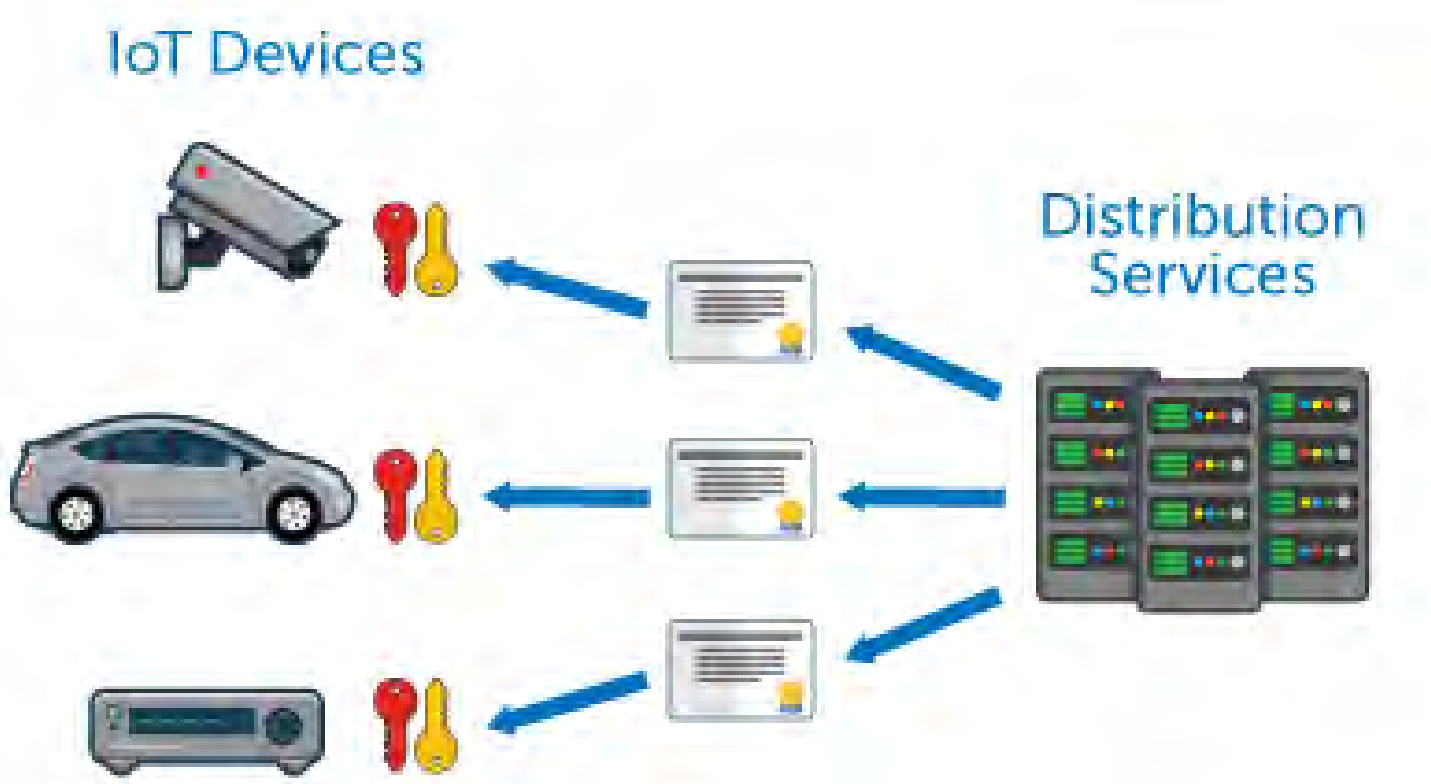


Smart Cities

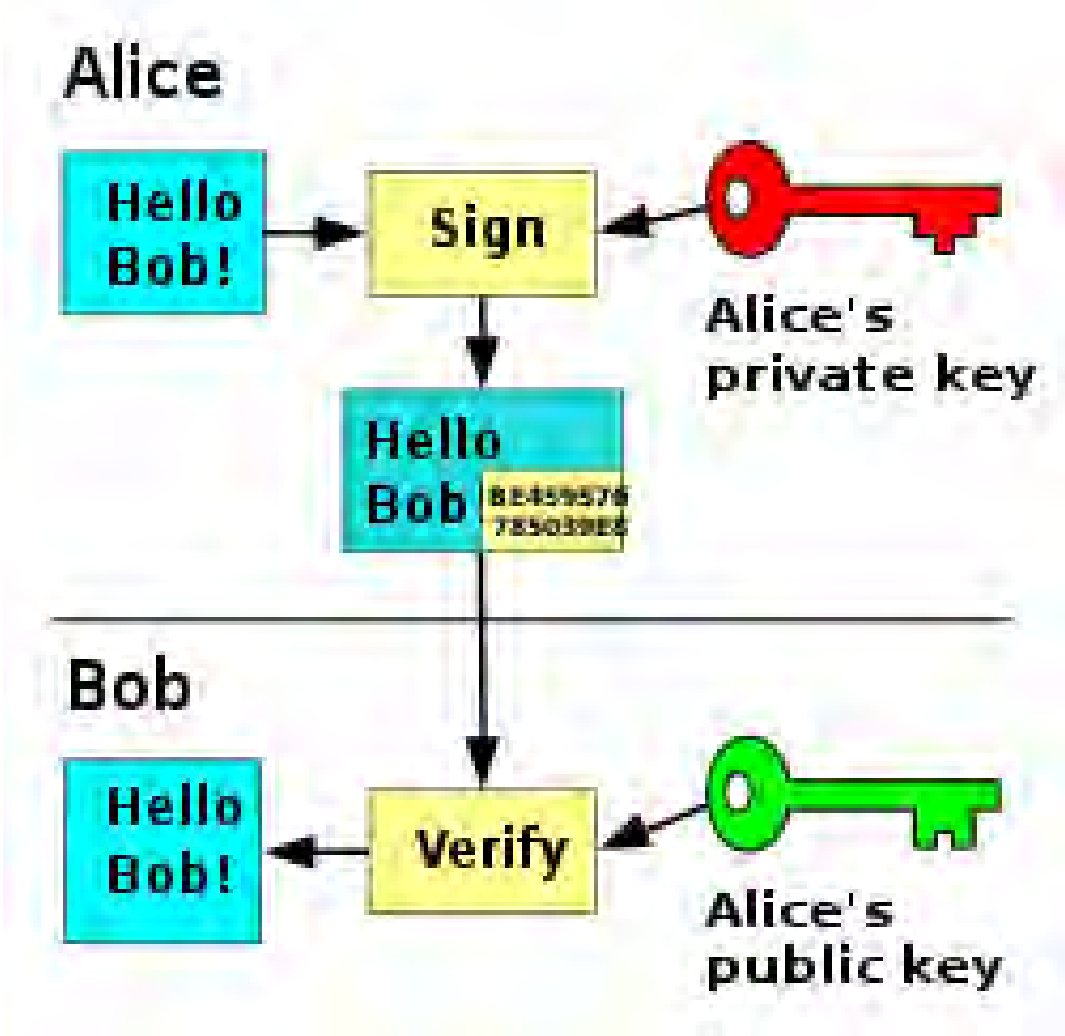
- Smart cities are built by the integration of several smart systems and technologies, such as smart sensor networks, smart meters, smart grids, smart homes, and smart vehicular networks.

Authentication

- Is the method of proving the identity of a user.
- One way to prove authenticate user is by using digital signature.

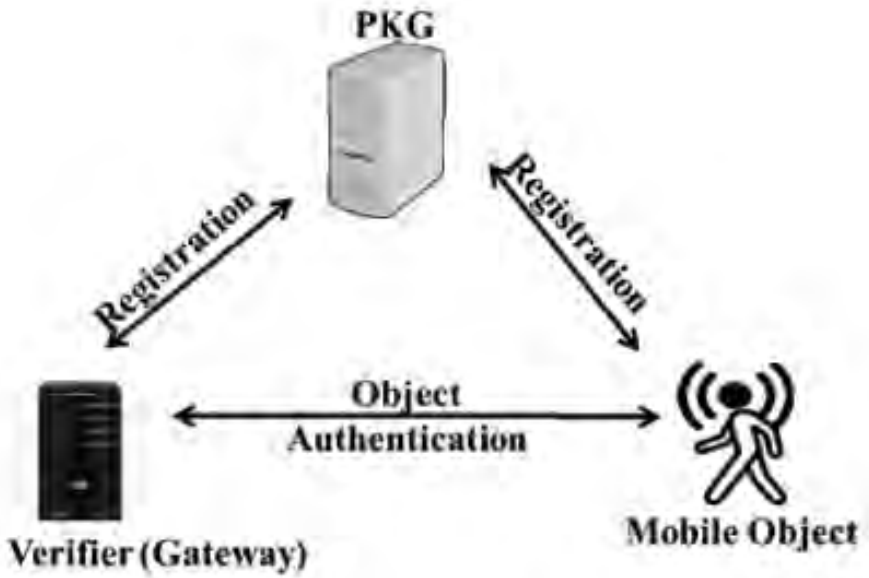


Public Key Cryptography



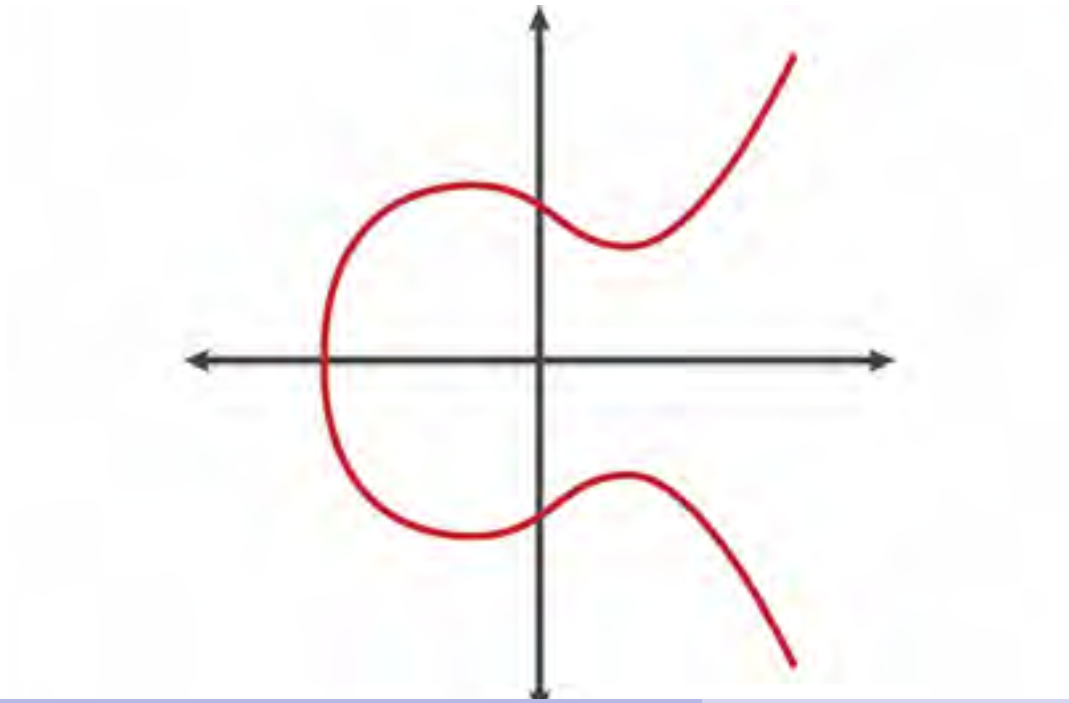
Identity-Based Signatures

- It is a type of public key cryptography.
- The public key is the identity of the user.
- The corresponding private key is issued by a trusted public key generator (PKG)



Elliptic Curve Cryptography

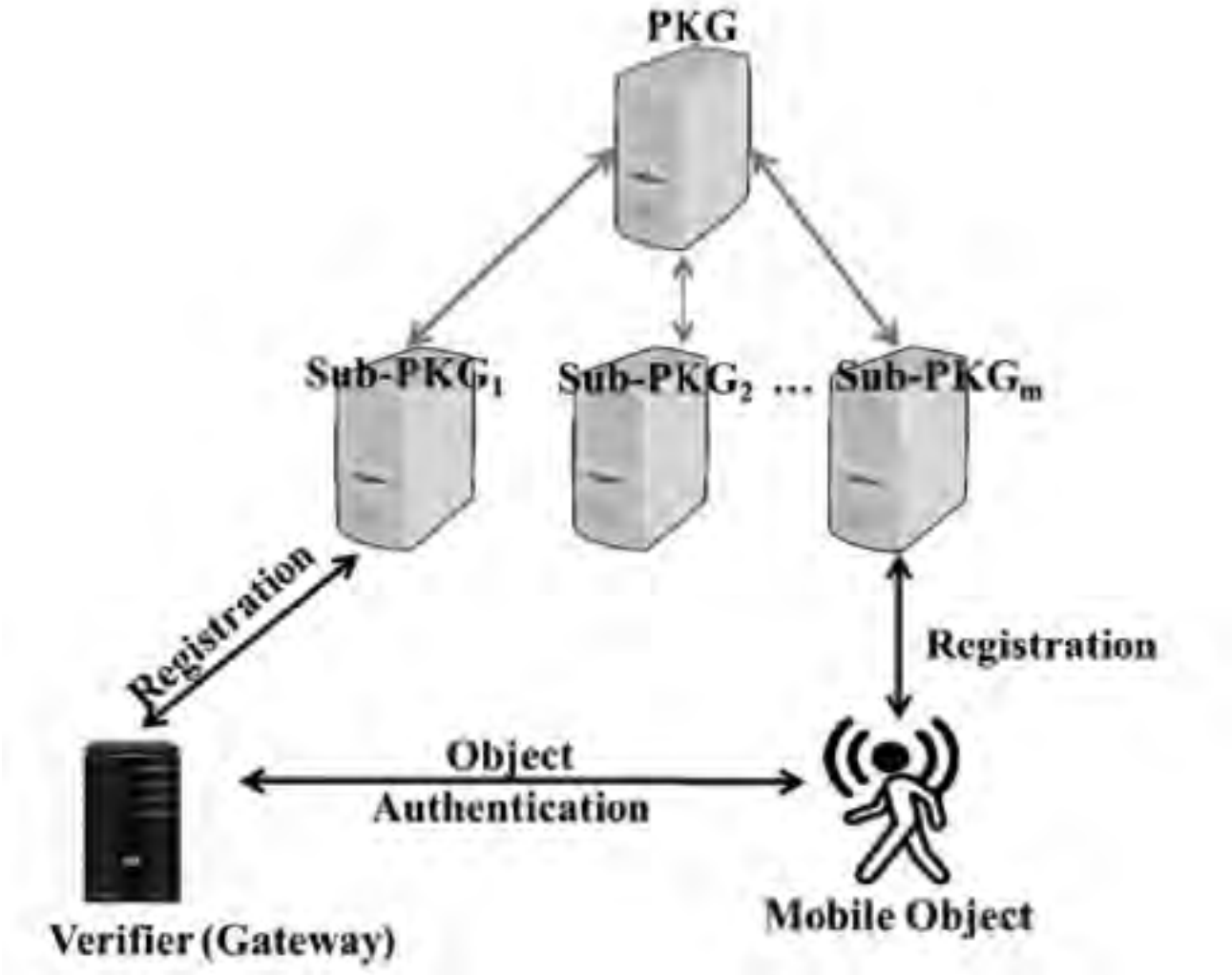
- It is an approach to public key cryptography.
- It is based on the algebraic structure of elliptic curves over finite fields.
- It allows smaller keys



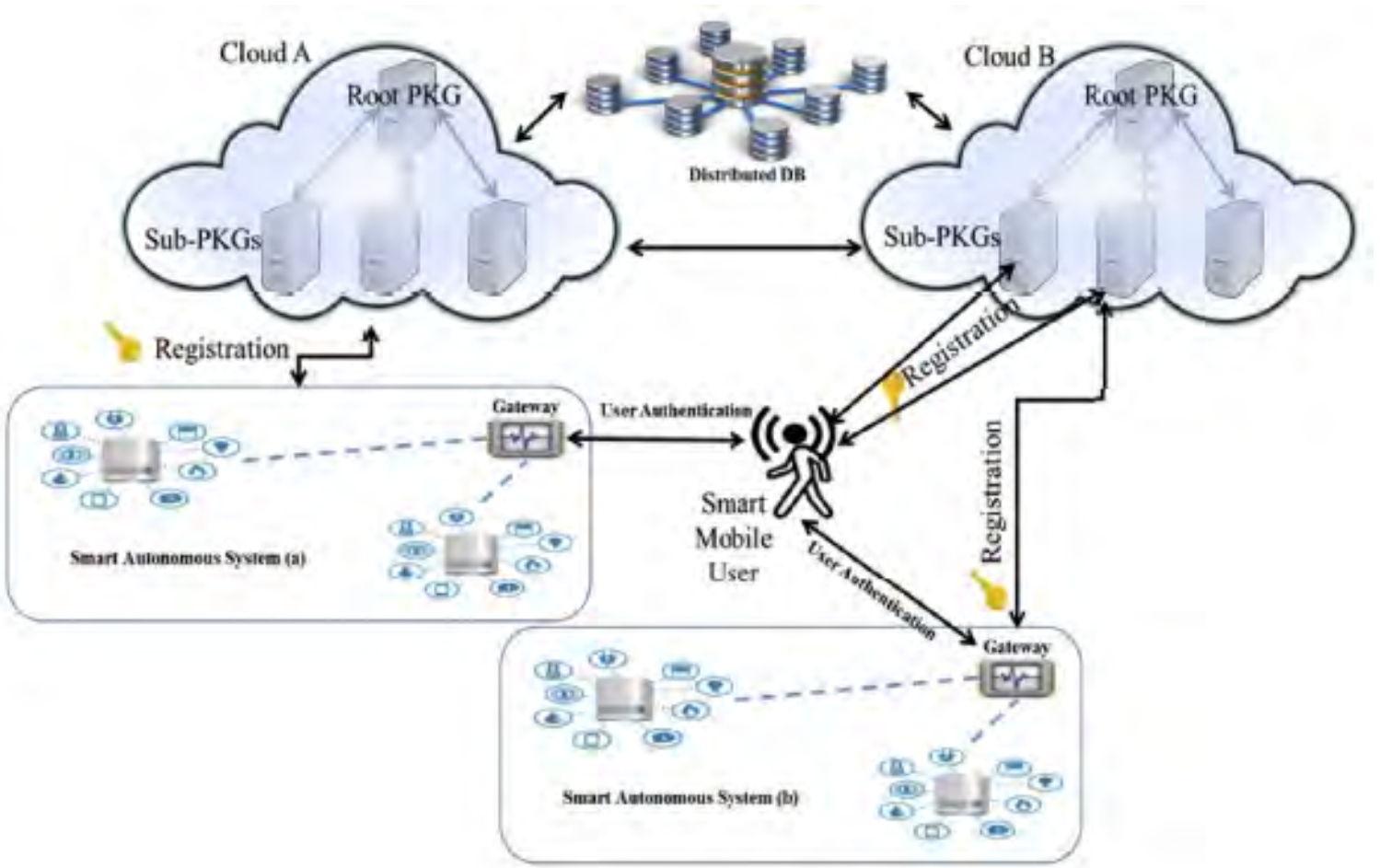
Challenges

- Scalability of IoT with large number of objects which are all connected together.
- Heterogeneity of the various objects, networks, and domains that already exist or expected to exist in the future.
- Mobility by allowing some objects to move between different networks while they still need to be authenticated in order to access resources that exist in these networks.
- Limited capabilities, such as storage and processing capabilities, of IoT constrained devices.

The Hierarchical Architecture

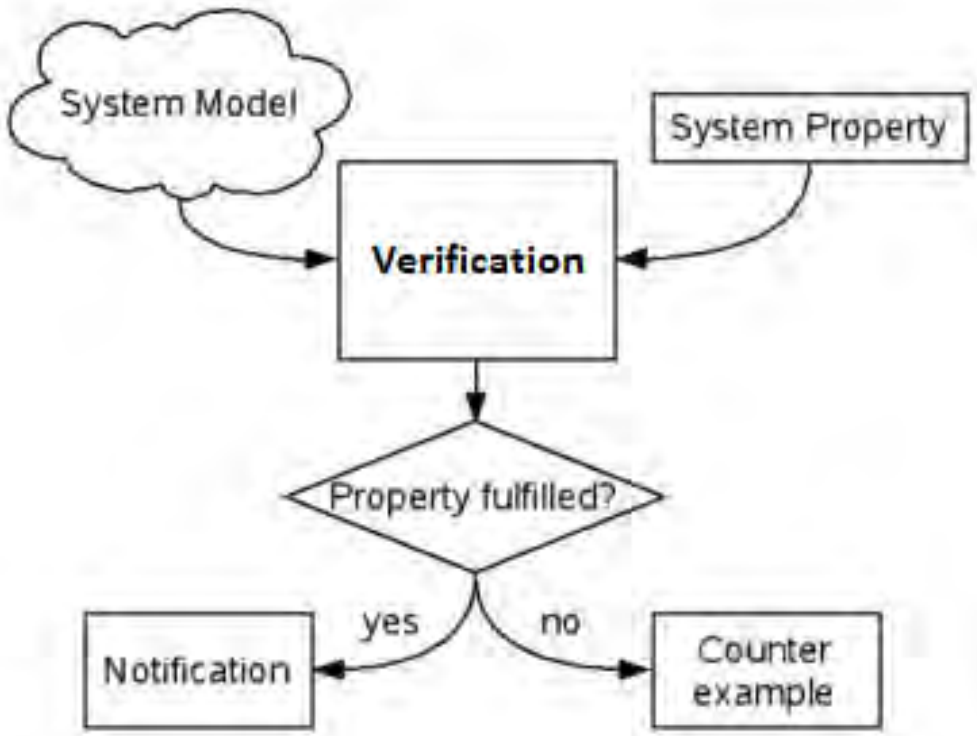


Generalized Hierarchical Architecture



Protocol Verification

- BAN logic is used to analyze the security of authentication protocols.



Security Analysis

- An adversary cannot compute the private key from the public information
- An adversary cannot link two previously sent signatures in order to calculate the private key.
- The proposed IBS protocol is safe against replay attack.
- The proposed IBS protocol is safe against impersonation attack.

Performance Evaluation

- The performance of the proposed protocol is evaluated based on the computation cost of each phase.