**CHAPTER-2**

**2INTRODUCTION**

As one of the most important entrances to kinds of information systems, authentication plays a prominent role in information system protection, which ensures the right user have access to the right system with the right identity[1-2]. Currently, the identity authentication technologies[3-8] are consist of 1)Password-based authentication. 2) Certificate-based authentication. 3) Biotechnology-based authentication, for instance, face, fingerprint or sound recognition. As is known to all, the password-based authentication system stores the hash value of user’s password in the database, and compares the current new password hash values with the stored hash of the original password. If they are consistent, the authentication is passed, otherwise the authentication will be rejected. Although the password-based authentication method is easy to achieve, some serioussecurity problems are existed, such as the brute force crackingand the dictionary attack. In order to ensure the identity information is not tamperedand destroyed, Certificate-based authentication uses digitalcertificates in the authentication process, which is regarded asan extremely secure and reliable way. Digital certificate caneffectively solve the problem of identity authentication in thenetwork world by binding the identity information and relatedkey of certificate holder. As the basic architecture of thedigital certificate, Public Key Infrastructure(PKI) providesidentity establishment and authentication mechanism in thenetwork through digital certificates management, whichallows users to use encryption, decryption technology anddigital signature technology in various application scenarioseasily[1-3,7-9]. And Biotechnology-based authentication collects users' biometric information, such as fingerprint, face, iris, voiceprint and so on, and compares them for identityinformation security. Biometric-based identification technology has many advantages over traditional identity authentication, for example, confidentiality, convenience, good anti-counterfeiting performance, not easy to forge orsteal, carry around and use anytime and anywhere. However, the collection of biometric information is difficult. If theinformation is not encrypted, it may cause the leakage ofprivate information [4-10]. Unfortunately, the current traditional authenticationmethods, such as the ones introduced above, are centralizedschemes, which are weak and single-side with poor faulttolerance and reliability. Meanwhile, they have the followingdisadvantages[1-2,10-12]: 1) The current single authentication has the hidden dangerof single point failure, which is easy to be the target of theattacker, because the attacker can easily forge identity andothers to implement the invasion. 2) Blindly trust the authentication agency will bring majorsecurity problems, the authentication agency may issue thewrong type of certificate, and are vulnerable to hacking,forgery, and falsification of digital certificates. 3) It is difficult for a single organization to provide multipletypes of identity data on which comprehensive multi-factorauthentication depends. Moreover, when a single organizationis attacked, its corresponding local multi-factor identity datacan still be leaked[8-10]. Obviously, in the centralized network, all managementrights are gathered in the central node, which bears a huge riskbecause of the significant responsibility given.

* 1. **LITERATURE SURVEY**

# Title: EAC: A Framework of Authentication Property for the IOTs

# Author: [Licai Liu](https://ieeexplore.ieee.org/author/37085491490); [Lihua Yin](https://ieeexplore.ieee.org/author/37086410805); [Yunchuan Guo](https://ieeexplore.ieee.org/author/38105681700); [Bingxing Fang](https://ieeexplore.ieee.org/author/38185478300)

**ABSTRACT**: Authentication is a slick and important security property and its proposed formal definitions are not widely agreed upon. Moreover, these definitions cannot faithfully express the requirements of diverse security and privacy in the Internet of Things (IOTs). To solve these problems, we proposed a framework of authentication, which including three forms of authentication -- entity authentication, action authentication and claim authentication -- and formalized each definition by using CSP for IOTs in this paper. We show that the framework can easily express different security requirements of IOTs and verify authentication of protocols.

# 2.Title: Anonymous Secure Framework in Connected Smart Home Environments

# Author: [Pardeep Kumar](https://ieeexplore.ieee.org/author/38583528800)

# ABSTRACT: This paper proposes an anonymous secure framework (ASF) in connected smart home environments, using solely lightweight operations. The proposed framework in this paper provides efficient authentication and key agreement, and enables devices (identity and data) anonymity and unlinkability. One-time session key progression regularly renews the session key for the smart devices and dilutes the risk of using a compromised session key in the ASF. It is demonstrated that computation complexity of the proposed framework is low as compared with the existing schemes, while security has been significantly improved.

# 3.Title: A Provably Secure Mobile User Authentication Scheme for Big Data Collection in IoT-Enabled Maritime Intelligent Transportation System

# Author: [Khalid Mahmood](https://ieeexplore.ieee.org/author/37300228600)

**ABSTRACT:** The emergence of contemporary technologies like cloud computing and the Internet of Things (IoT) has revolutionized the trends in the cyber world to serve humanity. There are plenty of applications in which they are being used, especially in smart cities and their constituents, Maritime Transportation System (MTS) is one of them. The IoT-enabled MTS has the potential to entertain the growing challenges of modern-day ship transportation. Secure real-time data access from numerous smart IoT devices is the most critical and crucial exercise for Big Data acquisition in IoT-enabled MTS. Therefore, we have developed a Physically Unclonable Function (PUF) based authenticated key agreement solution to deal with this challenge. This solution enables the mobile user and IoT node to mutually authenticate each other via Cloud-Gateway before real-time data exchange and transmission in IoT-enabled MTS. The use of PUF in our solution brings invincibility against physical security threats. An inclusive security analysis under the assumption of the specified threat model is carried out to substantiate the security resilience of our solution. The conduct of our solution is realized through security features, communication, and computation cost and It has been observed that our solution achieves efficiency of 37.3% and 9.7% in communication and computation overhead, respectively. Moreover, the network performance effectiveness of our solution is demonstrated in NS3 implementation.

# 4.Title: Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System

# Author: [Shaoyong Guo](https://ieeexplore.ieee.org/author/37592651400)

# ABSTRACT: As the great prevalence of various Internet of Things (IoT) terminals, how to solve the problem of isolated information among different IoT platforms attracts attention from both academia and industry. It is necessary to establish a trusted access system to achieve secure authentication and collaborative sharing. Therefore, this article proposes a distributed and trusted authentication system based on blockchain and edge computing, aiming to improve authentication efficiency. This system consists of physical network layer, blockchain edge layer and blockchain network layer. Through the blockchain network, an optimized practical Byzantine fault tolerance consensus algorithm is designed to construct a consortium blockchain for storing authentication data and logs. It guarantees trusted authentication and achieves activity traceability of terminals. Furthermore, edge computing is applied in blockchain edge nodes, to provide name resolution and edge authentication service based on smart contracts. Meanwhile, an asymmetric cryptography is designed, to prevent connection between nodes and terminals from being attacked. And a caching strategy based on edge computing is proposed to improve hit ratio. Our proposed authentication mechanism is evaluated with respect to communication and computation costs. Simulation results show that the caching strategy outperforms existing edge computing strategies by 6%-12% in terms of average delay, and 8%-14% in hit ratio.

# 5.Title:  A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes

# Author: [Randa Almadhoun](https://ieeexplore.ieee.org/author/37086101354); [Maha Kadadha](https://ieeexplore.ieee.org/author/37085992576)

**ABSTRACT:** In this paper, we propose a user authentication scheme using blockhain-enabled fog nodes in which fog nodes interface to Ethereum smart contracts to authenticate users to access IoT devices. The fog nodes are used to provide scalability to the system by relieving the IoT devices from carrying out heavy computation involving tasks related to authentication and communicating with the blockchain. We describe system components, architecture and design, and we discuss key aspects related to security analysis, functionality, testing and implementation of the smart contracts. The full code of the smart contracts for authentication registry, lists, rules and logic is also made publicly available at Github.