Editorial Preface

Special Issue on Security Mechanisms

G. Geetha, Lovely Professional University, Punjab, India

Security Mechanisms are features designed to detect, prevent, or recover from a security attack. This special issue invited papers to bring out the recent advancements in the field of security mechanisms including Personnel: Access Tokens, Biometrics, Physical: Integrated Access Control, Managerial: Security Education, Data Networking: Encryption, Configuration Control, Software and Operating System: Testing, Evaluation, Trusted O/S and various techniques including hardware implementation.

We thank all the authors who submitted their articles to this special issue and our special thanks and appreciations to all the authors whose eight articles are published in this issue. I wish, the contributors shall receive greater visibility and impact through this research publication.

The first article by Ranjeet Kumar Singh et. al., on hybrid concept of cryptography and dual watermarking provides multi level security in terms of data authentication in comparison to existing image data security approaches.

The second article is by Gautham Kumar et. al., on secure and robust telemedicine using ECC on radix-8 with formal verification. The authors have simulated application scenario for telemedicine on radix-8 scalar multiplication without precomputed operations for ECC thus reducing the complexity.

In the third article Arun Malik et. al. has presented a comprehensive identify authentication scheme for providing security in vanet using asymmetric encryption that facilitates the authentication for Vehicle-to-Infrastructure V2I and inter RSUs. The proposed algorithm outperforms the existing algorithms on the basis of communication overhead, latency and packet delivery ratio.

In the fourth article by Geetanjali Rathee et al. Diffie Hellman elliptic curve technique is used over Wireless Mesh Network where the data is propagated through multiple hops to destination node.

The fifth article by Gulshan Kumar et. al. proposed a Network Intrusion Detection System using packet filtering honeypots with snooping agents. The proposed method is validated based on the parameters like throughput, network load, queueing delay and retransmission attempts.

The sixth article by Rajeev Sobti et. al evaluated the performance of SHA-3 final round candidate algorithms on ARM Cortex M4 processor. They found that Blake algorithm is the best choice for all message digests irrespective of input sizes on ARM Cortex M4 processor. Skein is the second alternative where high security margin is required.

The seventh article by Rajni Mohana describes a three-step approach for successfully detecting rewriting attacks. The proposed model also concludes that the increase in the length of the SOAP message with tags is independent of the time required for encryption and decryption.

In the eighth article, the authors Puneet Kumar Kaushal et. al. examined the resistance of Tiny Encryptiion algorithm using coincidence count attack and bit sum attack. They also introduced an algorithm based on the concepts of coincidence count and bit sum.

We hope this special issue would kindle interest of several researchers in the field of cryptography and network security.

Dr. G. Geetha
Guest Editor, IJISP