A Systematic Review on Digital Signature Verification and Modern Development

HMSS Dissanayake, RGC Upeksha, TL Weerawardane

Department of Computer Science, Faculty of Computing, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka

Abstract. A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Digital signature techniques have considerably grown with the advancement of computer and network technologies, from single signature and single verification techniques to multi-signature approaches. To increase the data security and authenticity of transmitted data, further studies on digital signatures should be conducted. In this review paper, systematically analyses the common and modern algorithms for digital signature verification. Elgamal Scheme and Schnorr Scheme are used as common algorithms. Bio-Gamal Algorithm, Hyper Elliptic Curve Digital Signature Algorithm, Eigen-signature, XTR System, IDStack, ISRSAC, and Dynamic Signature Verification are used as modern algorithms. As a result, the bio-gamal system is ahead when compared to the Elgamal system. XTR system is ahead when compared with the RSA and ECC systems. When comes to offline signature verification, Eigen Signature is recommended. IDStack architecture is helpful when sharing a document like pdf. Apart from that, it was noticed chain verification signature scheme which developed by using ECC and ISRIAC algorithm which has developed to improve the security of the RSA algorithm. All these algorithms and methods can use for improving the level of security on Online data transfer, Offline signature verification and Document or file transfer by managing the tools and algorithms. A performance analysis has been carried out in this study along with the literature review. In addition, it is possible and recommended to create new algorithms and systems by using or combining the current systems for digital signature and verification. it will help reduce the disadvantages of existing algorithms.

Keywords: *digital signature, Cyber Security, Database security, digital signature verification.*