Mini Review
Volume 15:9, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

White Box Cryptographic Algorithms Using Enhanced Encryption Methods in Virtual Biometric Authentication

Evison Foster*

Department of Information Science, University of Toronto, 27 King's College Cir, Toronto, ON M5S, Canada

Abstract

Because of its growing popularity, the use of a piece of technology known as a digital signature is becoming more common. Its primary responsibilities include detecting and preventing unauthorised changes to the data as well as verifying the identity of the signature. Some of the possible applications for digital signatures include the signing of legally binding contracts, the protection of software updates and the use of digital certificates to ensure the security of online business transactions. Digital signatures have the potential to be used in a wide range of other situations. Because it uses public channels, a public key white box is the single most important example of a public key white box. This is in addition to the process of establishing keys through insecure channels, which is also a critical component of the equation. It is critical for ensuring the security of monetary transactions that take place over open or insecure networks. Digital signature techniques are commonly used in white-box cryptographic protocols. This allows for the provision of services like entity authentication, authenticated key transfer and key agreement.

Keywords: Cryptographic algorithms • Internet of things • Lightweight cryptography

Introduction

In some cases, the functionality of digital signatures is comparable to that of handwritten signatures. They, in particular, provide a way to ensure that a message sent to a specific user is genuine, in the sense that it came from the same person who claimed to be the one responsible for sending the message. This is because they provide a method for verifying the identity of the individual who claimed to be the person responsible for delivering the message. Nonetheless, they offer a much higher level of functionality. A large number of devices with limited capabilities are connected to the internet in a new computer environment. The network allows the devices to communicate with one another, which improves the user experience. The Internet of Things (IoT) technology of today enables a large number of objects with limited resources and communication capabilities to communicate, compute and make decisions within a communication network. In order to deal with this new environment, it is critical that the security of limited end nodes be maintained. If adequate protection services are not in place, any and all private information is vulnerable to being compromised, accessed and disclosed. Because of the dramatic increase in system vulnerabilities, attacking information systems has become much easier.

Literature Review

This increases the likelihood of Cyberattacks. An increasing number of businesses are experiencing problems that put their work at risk due to a lack of high-end security; the root cause of these problems is a lack of resources. As technology advances and more people gain access to more marketplaces, it is becoming increasingly important to safeguard information in order to ensure its confidentiality, integrity and availability. However, due to the limited resources of restricted devices, implementing appropriate cryptographic functionality on such devices is a difficult task. One of the most advanced approaches, "Lightweight Cryptography (LWC)," is capable of providing security services as well as the necessary level of privacy for devices that use it. LWC is a type of cryptographic technique or protocol that was created specifically for use in resource-constrained situations. Lightweight cryptosystems are the best option for preventing various types of malicious attacks and enforcing the four primary security requirements of confidentiality, availability, integrity and authentication when it comes to advanced communication technologies. This is because lightweight cryptosystems require the fewest resources. It is well understood that "Information Security" plays an important role in the new era of information technology [1-3]. This is required in order to address lightweight cryptographic primitives such as lightweight stream cyphers, hash functions and low-resource devices for Internet of Things environments adequately.

Individuals have spent a significant amount of time associating their identities with the documents that they sign using various signatures. Wills, contracts and other legal documents are examples of such documents. These signatures can be found on a wide range of different types of papers. During the Middle Ages, a nobleman would affix a wax seal to a document to ensure its authenticity. This would ensure the document's authenticity. It was widely assumed that the noble was the only one who possessed the skills required to successfully recreate the emblem. This assumption, however, proved to be incorrect. Credit card slips must be signed on the reverse side when used in current transactions [4,5].

Discussion

It is the salesperson's responsibility to validate the signature by comparing it to the signature already imprinted on the card. As internet commerce and digital documentation have grown in popularity, these strategies have become obsolete and inadequate. In today's fast-paced technological world, the importance of information and communication systems is growing in tandem with the increasing importance and volume of data that is transmitted in order to reduce operational costs and provide better services. This is because more data is being transmitted, which means more data needs to be transmitted. This is due to the increased amount of data that is being delivered in order to achieve these goals. The increase in the relevance of this phenomenon is directly related to the increase in the amount of data sent and this correlation is a one-to-one relationship. Unfortunately, the vulnerability of systems and data is growing as a result of an expanding range of threats [6-7].

***Address for Correspondence:** Evison Foster, Department of Information Science, University of Toronto, 27 King's College Cir, Toronto, ON M5S, Canada, E-mail: EvisonFoster3@yahoo.com*

Received: 07 September, 2022, Manuscript No. jcsb-22-83699; **Editor assigned:** 09 September, 2022, Pre QC No. P-83699; **Reviewed:** 21 September, 2022, QC No. Q-83699; **Revised:** 26 September, 2022, Manuscript No. R-83699; **Published:** 03 October, 2022, DOI: 10.37421/0974-7230.2022.15.433

These risks include system and data destruction, modification and theft, as well as unauthorised data access and exploitation. All other data and information security processes are built on top of the white box concept, which serves as the foundation for their development. Because it makes the exchange of information easier and more convenient, the internet has been directly responsible for a fundamental shift in the way business and transactions are conducted. This shift has occurred as a direct result of the fact that it allows for a faster flow of information. Digital signatures are another example of a "white box" cryptographic method. A physical signature can be converted into an electronic signature, known as a digital signature. A handwritten signature is analogous to a digital signature in the realm of digital transactions. To be valid, a digital signature cannot be a static image; rather, it must be generated dynamically based on the information in the document being signed. One of the most significant differences between a handwritten signature and a digital signature is this. At any time, a digital signature can be changed. It is used to confirm that a person pledged something that he or she cannot take back later.

The promise is irrevocable. When working with electronic documents, you must use a system that can perform the same functions as the electronic documents themselves. The use of digital signatures to confirm and verify the authenticity of electronic documents is becoming increasingly popular. When a digital signature algorithm is used, the output is a string of ones and zeroes that, when combined, form what is known as a digital signature. The process of determining whether or not the information in the document is correct is known as "validation." Authentication is the process of verifying the identity of the person who sent a document. The primary applications for the exchange of digital signatures are e-mail and other forms of electronic communication. Examples include software distribution and other applications that must ensure data integrity and authenticate the source of the data. Other applications that require digital signatures include those that require data authentication.

Digital signatures may also be used in other applications that require the origin of the data to be verified, which digital signatures can do. Wireless protocols, such as HiperLAN/2, each have their own set of security levels and digital signatures are used to authenticate users. When data corruption or an unauthorised client is discovered during the process of data forwarding over dispersed servers, the servers that are performing poorly can be identified at the same time. This identification can happen at any time. This method saves a significant amount of time and effort when optimising the number of cloud server requests, which eventually leads to congestion management between cloud servers.

Conclusion

End-to-end security in the cloud storage environment is undoubtedly a difficult task because malicious users can find a way to prevent alert messages from being sent to the owner of the cloud storage organization during unauthorised file access. End-to-end security is therefore not always possible. The system is capable of integrating storage with secure forwarding and online alert notification to the service provider when unauthorised files are modified or accessed by malicious hackers during a value-added online exchange of forward data over the cloud. The combination of secure forwarding and online alert notifications makes this possible. Even though the results of the experiments show that the proposed scheme performs better in terms of throughput and storage server cost, there are still some issues that need to be addressed. These issues include ensuring the data's integrity, preserving user anonymity and determining how quickly users can retrieve the data. A digital signature can also be used to ensure that the information signed has not been altered after it was signed.

Acknowledgement

None.

Conflict of Interest

Authors declare no conflict of interest.

References

1. Yeom, Yongjin, Dong-Chan Kim, Chung Hun Baek and Junbum Shin. "Cryptanalysis of the obfuscated round boundary technique for whitebox cryptography." *Sci China Inf Sci* 63 (2020): 1-3.
2. Marin, Leandro. "White box implementations using non-commutative cryptography." *Sensors* 19 (2019): 1122.
3. Feng, Qi, Debiao He, Huaqun Wang and Neeraj Kumar, et al. "White-box implementation of Shamir's identity-based signature scheme." *IEEE Syst J* 14 (2019): 1820-1829.
4. Visconti, Andrea and Federico Gorla. "Exploiting an HMAC-SHA-1 optimization to speed up PBKDF2." *IEEE Trans Dependable Secure Comput* 17 (2018): 775-781.
5. Light, Roger A. "Mosquitto: Server and client implementation of the MQTT protocol." *J Open Source Softw* 2 (2017): 265.
6. Lee, Seungkwang, Taesung Kim and Yousung Kang. "A masked white-box cryptographic implementation for protecting against differential computation analysis." *IEEE Trans Inf Forensics Secur* 13 (2018): 2602-2615.
7. Goubin, Louis, Pascal Paillier, Matthieu Rivain and Junwei Wang. "How to reveal the secrets of an obscure white-box implementation." *J Cryptogr Eng* 10 (2020): 49-66.

How to cite this article: Foster, Evison. "White Box Cryptographic Algorithms Using Enhanced Encryption Methods in Virtual Biometric Authentication." J Comput Sci Syst Biol 15 (2022):433.