International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

An Approach to Multi-Layer Authentication in E-Signature

Sagar Dhawale[1], Savita Sheelavant[2]

PG Student, Department of MCA, Rastreeya Vidyalaya College of Engineering, Bengaluru, Karnataka, India[1]

Assistant Professor, Department of MCA, Rastreeya Vidyalaya College of Engineering, Bengaluru, Karnataka, India[2]

ABSTRACT: Information security, is that the application of protective data by mitigating data risks. It's a part of data risk management. It generally involves preventing or a minimum of reducing the chance of unauthorized/inappropriate access to information. The work proposes an idea of integrating e-signature with biometrics and system credentials so that authentication will have multi-tire authentication and legally verifiable. It gives the solution to the problem of depending only on a minimal layer of authentication given by an application to sign electronically. This proposed idea of integration of a few authentication methods will attract users to use e-signatures.

KEYWORDS: E-Signature; Key generation;Verification; Private Key;HWID- Hardware Identification

I. INTRODUCTION

An electronic signature refers to information in electronic type, that is logically related to different data in electronic form and that is employed by the individual to sign. This sort of signature provides legal standing as a written signature as long as it sticks to particular regulation it had been created under. There is a great deal of various applications accessible that permit you to look at a signed and saved .pdf. Adobe is far and away the dominant player within the market. The E-signatures are championed by several players that the general public distrusts, as well as national security agencies, enforcement agencies, and client promoting firms.

The Security requirements which are necessary for any internet communication are Integrity,Confidentiality, Authentication, Availability, and Nonrepudiation. E-Signatures are far more secure compared to physical signatures which are simply replicated or "forged". The system behind the e-signature is tough so it is not possible to manipulate them. As the security ismaintained with E-Signatures and also the number of points of interest connected with putting away reports electronically.

II. LITERATURE SURVEY

G. Saha, et al focuses on the aim of this paper is to solve the problems related to integrity and authenticity of e-business application solution in Indian perspective.The application of digital signature has made the solution secure, authentic, and accountable. It's advisable to own an in depth study of the present model before the designing phase. This minimises the requirement for Business Process Reengineering (BPR) an analogous approach will be extended for e-Governance system in Indian perspective for state offices wherein signed approvals from the competent authority may be a mandatory process [1].

Tianhuang, Chen & Xiaoguang, Xuconcentrates on e-signature technology in the application of e-commerce, based on thee-signature algorithm, that is an DSA algorithm idea.The DSA algorithm used in this paper works well to address the issues of e-signatures supported simulation. This paper discusses modern e-commerce security issues and the way to use a digital signature, a really powerful tool to unravel practical problems [2].

L. Zhu and L. Zhu illustrate an e-signature algorithm, employing a combined technology of e-signature, time stamp, digital watermarking, is given within the signature algorithm, a digital watermark embedding algorithm supported wavelets remodel module most is meant using this algorithm, the signature information is commonly included into the signature image as a watermark, improving the signature information safety, hidden and anti-offensive compared with a traditional electronic signature solution. [3].

The predominantly strong and weak aspects of signal transmission and processing under external and internal attacks from the position of reliability for the marine industry are investigated in this paper. The authors S. G. Chernyi, et alalso proposes a most secure way of storing the private key - storage ona smart card. To use a smart card, the user needs not only to possess it but also to enter the PIN -code, that is, it seems two-factor authentication. Thereafter, thedocument is signed or the hash is transmitted to the card processor performs it's signing the hash and transmits the signature back [4].

Wang, Guilinhas proposed another advanced signing protocol convention. Based on the based on RSA digital signature model the trusted party is possibly included when one party is cheating the other or is intruded. In this paper,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

in light of the standard RSA signature plot, the author proposed another advanced agreement marking convention that licenses two possibly uncertain parties to trade their computerized sign to go for an effective and secure way. As same as the present RSA-based algorithm, the new convention is reasonable, i.e., two parties get or don't get the other's advanced mark at the same instance, and furthermore the believed outsider is basically required in unusual cases that happen at times [5].

The authors Dr. Ali Al-Zubi and Dr. Bassam Al-Trawneh talks regarding the authentic legal of electronic signature within the Jordanian law, and legal provision during this space. Then the topic of legal and technical issues that raised the sensible application of the law [6].D.Shiva Rama Krishna, et al introduces the thought, characteristics, connected technologies of digital signatures, and also the current analysis state of many sorts of digital signature [7].

Kaur, Ravneet & Kaur, Amandeepdescribes the various key factors of e-signature with the working of digital signature, through various methods and procedures involved in signing the information or message by using an e-signature. It introduces algorithms utilized in e-signatures [8].

Payel Sahaillustrates aboutE-Signature schemes are commonly employed in cryptographic protocols to provide services like entity authentication, authenticated key transport, and authenticated key agreement. This architecture is expounded to Cryptographic Algorithm and Hashing Algorithm. This Research paper presents a comprehensive study of E-Signature and its Algorithm for Internet Security purpose [9].

H. Tao, et al focuses on a very important problem that the safety of the e-commerce system has become one in all the important issues and the main blockagewhich constraints the event of e-commerce is distinguished. The inadequacy in present e-signature process is pointed out. Supported digital encryption and knowledge hiding, and some realizing schemes for the techniques of are elaborated, a clever new idea to escort the selection among the e-signature strategyhaving a safety/speed ratio e-signature strength theory is proposed, and also the developing management of an e-commerce security [10].

Jakisch G focuses onE-Signature verse e-Identity highlights the precise issues public authorities' area unit confronted with by their conversion to e-Government. By suggests of the authorthe analogy between traditional and digital versions, the issue area addressed and doable solutions guided [11].Y. Ren, et alfocuses on the usage of mobile devices enable conducting electronic transactions involving direct E-signature on such devices [12].

III. EXISTING PROCESS OF E-SIGNATURE

The existing process involved with the e-signature process:

- *Key generation* –this process provides a private key and its public key.
- *Signing* –produces a signature upon acquiring a private key and the datawhich is signed.
- *Verification* – This process checks for the authenticity of the message by verifying it with the signature and its public key.

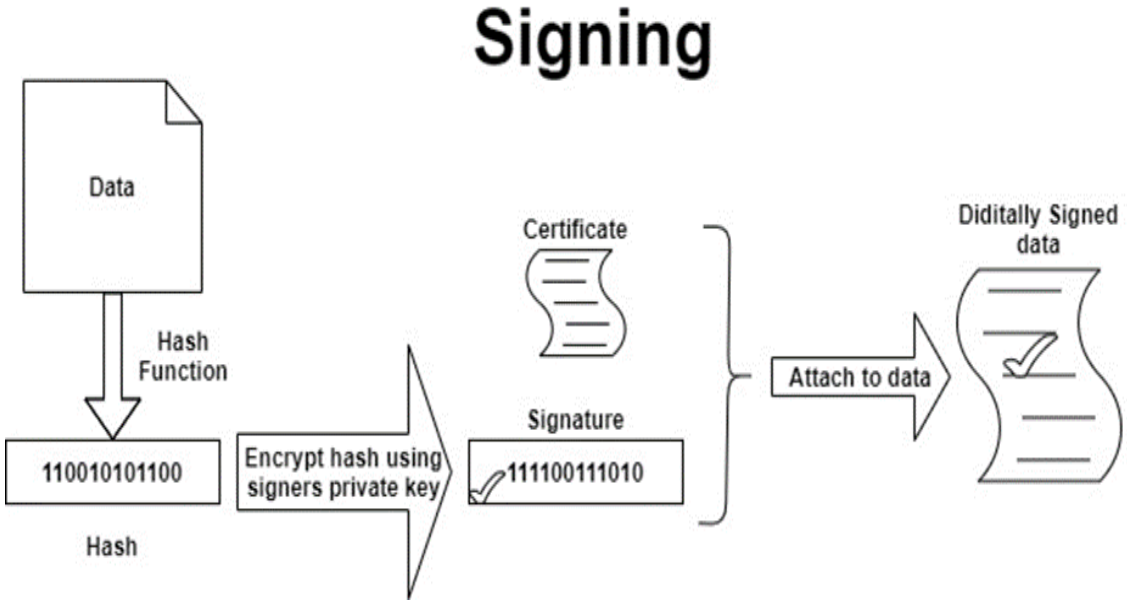

Fig.1.Existing Process of Signing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

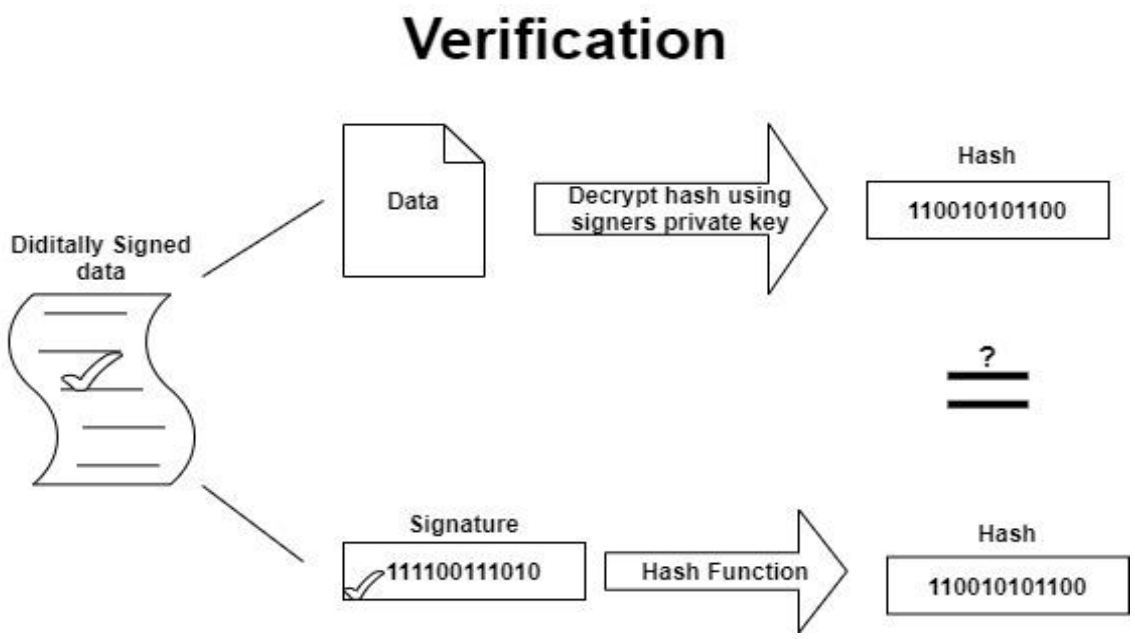

Fig.2.Existing Process of Verification

In Fig 1 and Fig 2, the process of digital signing needs that the signature generated by each the mounted message and private key will then be certified by its to public key. using these cryptologic algorithms, the user's signature cannot be replicated while not having access to their non-public key. A secure channel isn't usually needed. By applying uneven cryptography ways, the digital signature method prevents many common attacks wherever the wrongdoer tries to achieve access through the subsequent attack ways. E-signature technology permits the recipient of the given signed message to verify its real origin and its integrity. The method of e-signature verification is purposed to establish if a given message has been signed by the non-public key that corresponds to a given public key.

IV. MERITS OF IMPLEMENTING E-SIGNATURE

Along with facilitating business processes and preventing the forgery of critical messages and documents, the use of digital signing provides additional validation benefits. In the case where an assurance is needed that a message or an accompanied document has not been altered during transmission, a digital signature will prevent unknown alterations from going unnoticed. If the digitally signed content is changed, the e-signature will be invalidated, therefore alerting the sender and receiver of a violation. This is because the applied cryptographic functions will prevent a new and valid e-signature from being created for that data.

When non-repudiation is allowed, the sender cannot reject digitally signing the data. The receivers who gain unauthorized access to the data also are prevented from establishing a fake signature. Most non-repudiation processes provide a time-stamp that cannot be changed and supply evidence of the e-signature within the event that the private key has been altered.

V. EXISTING LIMITATIONS OF E-SIGNATURE

In the process of e-signature, there is a hidden danger which is called " interception reading" because the sender sent the digital signature and the message to the receiver simultaneity, however, the message was not taken any encryption; So that the digital signature process can only authenticate the identity of the sender, prevent from denying and detect the message being tampered with. But if there is a third-party intercept the message and reads it (It means that the third-party only reads the content of the message, but do not make any alteration on the content). In transmission, the message in the plaintext will leak out. But both the sender and the receiver are not aware of it completely, so the occurrence of this event will bring huge losses to the sender and the receiver.

Not all electronic signature vendors provide enough security for digital transactions. The basic kind of e-signature offers no security against meddling, whereas others provide some basic tamper protection. The process verification of e-signature takes lot of time. So, the speed of communication can cut back. When the e-signature is notauthenticated by

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

the public key, the receiver will mark the document as invalid but he doesn't recognize whether or not the data was corrupted or the false private key was used.

VI. PROPOSED APPROACH TO MULTI-LAYER AUTHENTICATION

Fingerprint, face, hand, voice, iris, and other biological and behavioral features are commonly used to identify or verify individuals. When executing the identification process, the biological signature of a given individual is compared to many other signatures, stored in a database.

HWID- Hardware Identification, a security measure employed by Microsoft during the activation of the Windows software package. As a part of the merchandise Activation system, a singular HWID range is generated once the software package is initially put in. The HWID identifies the hardware elements that the system is using, and this range is communicated to Microsoft. every ten days and at each reboot the software package can generate another HWID and compare it to the initial to make certain that the software package remains running on the identical device. If the two HWID take to issue an excessive amount of then the software package will pack up until Microsoft reactivates the merchandise. Along with this the product id of the system can be used to uniquely identify a particular system.

As these authentication methods mentioned above are uniquely identified worldwide, combining system credentials and biometrics to authenticate e-signature in an application decreases the security concerns by keeping in mind the privacy of the signer must be maintained by encrypting these ID's

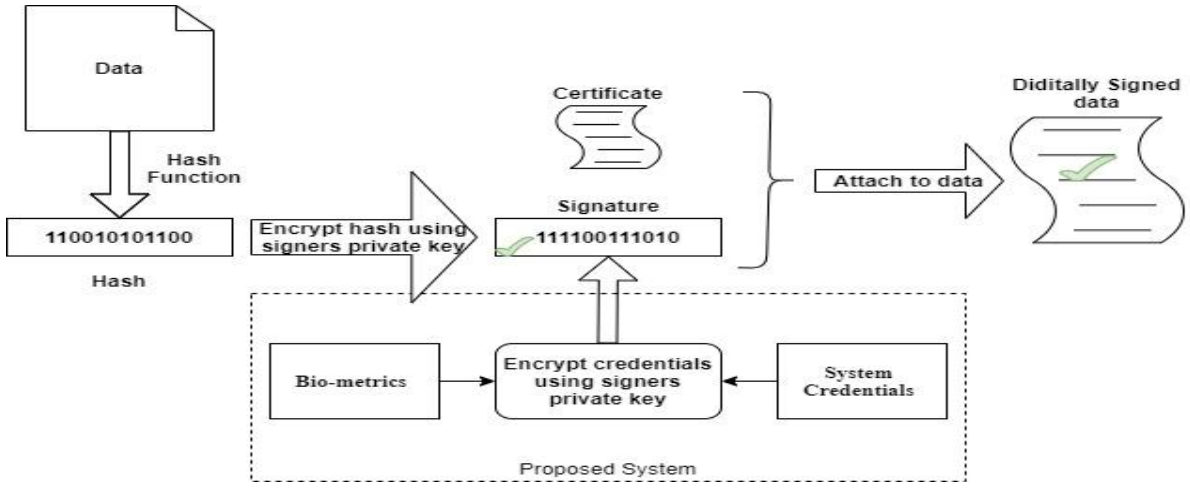

Fig.3.Multi-Layer Authentication

In the Fig 3, the signing process of e-signature, after encrypting the hash function using the signer's private key the signature is generated. In this step. The e-signature application can authenticate the signature by using the biometric sensor and the system credentials like HWID to further authenticate the signature. To maintain the privacy of the signer, both the biometric and system credentials can be encrypted using the signer's private key

VII. CONCLUSION

E-signatures play a vital role in providing security to documents and that can make an electronic transaction of those documents by using e-signatures in afixed manner. The digital equivalent of a handwritten signature or s a seal, but offering way more inherent security, an e-signature is meant to resolve the matter of interfering and imitation in digital communications.The implementation of the above proposed approach in improving the authentication of e-signature will help to attract users to use e-signatures. The existing system which has the limitation on no security against meddling, whereas others provide some basic tamper protection. These limitations can be minimized with this proposed layer of authentication by using already existing authentication system

REFERENCES

1. G. Saha, M. Desai, A. Ghosh and N. Saha, 'Digital Signature Modeling in E-Business,' IEEE 11th International Conference on e-Business Engineering, Guangzhou, 2014, pp. 350-354, doi: 10.1109/ICEBE.2014.67, 2014.
2. Tianhuang, Chen & Xiaoguang, Xu,'Digital signature in the application of e-commerce security'. 10.1109/EDT.2010.5496558,2010.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.194 |

||Volume 8, Issue 4, April 2020||

3. L. Zhu and L. Zhu,'Electronic signature based on digital signature and digital watermarking', 5th International Congress on Image and Signal Processing, Chongqing, 2012, pp. 1644-1647, doi: 10.1109/CISP.2012.6469828, 2012
4. S. G. Chernyi, A. A. Ali, V. V. Veselkov, I. L. Titov and V. Y. Budnik, 'Security of electronic digital signature in maritime industry', IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 29-32, doi: 10.1109/EIConRus.2018.8316861, 2018
5. Wang, Guilin, 'An abuse-free fair contract signing protocol based on the RSA signature', IEEE Transactions on Information Forensics and Security. 5. 158-168. 10.1145/1060745.1060807, 2010.
6. Dr. Ali Al-Zubi and Dr. Bassam Al-Trawneh,'The Electronic Signature and the Problems of Its Practical Applicable', International Journal of Humanities and Social Science Vol. 6, No. 12, 2016
7. D.Shiva Rama Krishna, Siva Rama Prasad Kollu , Ch.V.V.Narasimha Raju, 'Providing Information Security UsingPublic Key Cryptosystems', International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-3, Issue-3, 2015
8. Kaur, Ravneet & Kaur, Amandeep, 'Digital Signature', 2012 International Conference on Computing Sciences 295-301. 10.1109/ICCS.2012.25, 2012
9. Payel Saha, 'A comprehensive study on digital signature for internet security', ACCENTS Transactions on Information Security, Vol 1(1), 2016
10. H. Tao, Z. Qihai, Z. Le, L. Zhongjun and L. Xun,'An Improved Scheme for E-signature Techniques Based on Digital Encryption and Information Hiding', International Symposiums on Information Processing, Moscow, pp. 593-597, doi: 10.1109/ISIP.2008.47, 2008
11. Jakisch, G. (n.d.), 'E-Signature versus e-Identity: the creation of the digital citizen', Proceedings 11th International Workshop on Database and Expert Systems Applications. doi:10.1109/dexa.2000.875045, 2000
12. Y. Ren, C. Wang, Y. Chen, M. C. Chuah and J. Yang, 'Signature Verification Using Critical Segments for Securing Mobile Transactions,' in IEEE Transactions on Mobile Computing, vol. 19, no. 3, pp. 724-739, 1, doi: 10.1109/TMC.2019.2897657,2020
13. https://www.developer.com/java/ent/article.php/3092771/How-Digital-Signatures-Work-Digitally-Signing-Messages.htm
14. https://www.assuresign.com/blog/what-is-electronic-signature/