International Journal of Technology and Empirical Research

GNIT RESEARCH MANTRA Vol: 1, Issue: 1, September 2021

A Review on Security of Personal Credentials through Smart Technology using Advanced Digital Signatures

Sourjyadip Sarkar[1], Sourav Paul[2], Soumyajit Goswami[3], Souman Bej[4], Saikat Ghorai[5],Avali Banerjee[6], Suparna Biswas[7]

Department of ECE, Guru Nanak Institute of Technology, Kolkata, West Bengal, India

published online at https://gnitresearchmantra.in/

Abstract—In this era of modern technology and biometrics, digital signatures are being used to develop the security and authentication of an individual. It is used as an encrypting function for conventional systems for authenticity and integrity. The age of multimedia has brought many advantages in creation, edition and synthetization along with image authentication for new security purposes which includes human credentials such as signature and verification operations. It can be used in smart devices and can be upgraded to the next level of security system of one's personal and private credentials, taking in consideration with the authentication and biometrics. This kind of data can be used for advanced digital signatures with compact security facilities and can be also used for providing security to multi-national companies and their cyber securities including server firewalls. This paper is a review of the digital signatures that we can use in our daily lives and that can be implemented in human lives through smart mediums and can be connected to our securities, with all necessities and credentials secured at our fingertips.

Keywords—Arbitration Digital Signature; Biometrics; Elliptic Curve Cryptography; Image Authentication; Lightweight SCDSA; On Paper Digital Signatures.

I. INTRODUCTION

The Digital Signatures is the process by which the authenticity of many legal, financial, and other documents is being determined by the presence or absence of an authorized handwritten signature. The authentication of the handwritten signature ensures secure transaction with the cryptography system which enhances the specific algorithms that are based on a conventional encryption function along with certified conventional systems that can be implemented without any delay. The future of this world will be the digital technology based on hybrid cryptosystem in e-Government that would provide a guarantee for every information security.

The purpose of this paper is to show case and predict that how digital signatures will be very much valuable and important in the future. The authentications and securities that can be implemented by the advanced encryption of signatures and verifications, biometrics and image processing will be of higher-level securities. A combination of all the above-mentioned specifications can be accessed with smart appliances and the security of personal credentials will all be at their own authority.

II. LITERATURE SURVEY

Songnan Zhao et al. [1] proposed a hybrid digital signature based on arbitration digital signature system which includes AES, ECC and key distribution methods for confidential communication. They showed that the proposed system needs high security requirements suitable for e-Government authentication mechanism. Taekyoung Kwon et al. [2] proposed a simple practical method for biometrics based digital signature such as signature generation, combined with biometric encryption, fingerprint verification and bar code technology by exploiting tools where RSA can be applied without losing security. Rashmi Kasodhan et al. [3] also proposed a better way of security management from the above-mentioned techniques, just by implementing BioGamal algorithm also known as DNA algorithm in the security system for secure usage of digital signatures.

T.N. Shankar et al. [4] proposed the technique of Elliptic Curve Cryptography (ECC) which focuses on pairs of public and private keys for decryption and encryption of web traffic, and it is a context related to Rivest-Shamir-Adleman (RSA) cryptographic algorithm. This technique is very efficient for the future use in any context of digital signatures. Hong-Bin Zhang et al. [5] proposed the technique of image authentication and semi-fragile watermarking to verify the integrity, reality and the alleged source of a given image.

Muhammad Arif Mughal et al. [6] proposed the use of Lightweight SCDSA technique using IoT than DSA Schemes for less extensive complex number-based operations which reduces the computation and communication overhead along with better resilience and which can also be implemented in smart phone devices. Sajan Ambadiyil et al. [7] proposed on paper digital signature to verify the authentication of the identity of the sender and ensuring the content integrity in printed paper documents within a short period of time, which is essential for both the sender and receiver for an end-to-end encryption.

Ralph C. Merkle [7] described a digital signature system based on a conventional encryption function which has modest space and time requirements and a signature size. Selim G. Aki [8] discussed about digital signature schemes which are usually classified into one of two categories such as true signatures or arbitrated signatures. Ananthi Sheshasaayee et al. [10] discussed about the secure correspondence by detecting forgery or tampering of message.

III. ALGORITHMS USED IN DIFFERENT METHODS

A. Arbitration Digital Signature

1) Arbitration Digital Signature Scheme

An arbitration digital signature scheme is comprised between a three-way branch between a sender, arbiter and receiver. In an arbitrated signature there is most trust because the sender's message is sent to an arbiter to get authenticated before it is sent off to receiver. Hence, we can use arbitration digital signature scheme for future authentication in e-Government.

There are many schemes of arbitration digital signature:

- Scheme 1: private key (symmetric) encryption scheme, arbitrators can see the messages,

  S→A: M || EKsa [IDs || H(M)]

  A→R: EKar [IDs || M || EKsa [IDs || H(M) || T]]

- Scheme 2: private key (symmetric) encryption scheme, arbitrators can't see the messages.

  S→A : IDs || EKsr [M] || EKsa [IDs || H (EKsr[M])]

  A→R : EKar [IDs || EKsr [M] || EKsa [IDs|| H (EKsr[M])] || T]

- Scheme 3: dual key (public key) encryption scheme, arbitrators can't see the messages,

  S→A : IDs || EKRs [IDs || EKUr [EKRs[M]]]

  A→R : EKRa [IDs || EKUr [EKRs[M]] || T]

2) A New Hybrid Arbitration Digital Signature

In New Hybrid Arbitration Digital Signature, it is assertive that besides seeing the messages we can also do joint cheat. There are three pairs of public/private key – (KRs, KUs), (KRa, KUa) and (KRr, KUr) along with a private key (Ksr) which are being shared by the sender (S) and receiver (R), that are being used to implement signature in the scheme to encrypt certain messages. The scheme to be mentioned is as follows:

- S→A: IDs || C1 || C2 || C3.

  C1= EKsr [M];

  C2= EKUr [EKRs[H(M)]];

  C3= EKRs [IDs || H (IDs || C1 || C2)];

- A→R : C4 || C5.

  C4= IDs || C1 || C2 || T;

C5= EKRa [H(C4)];

B. Biometrics

1) Key Generation (T1 Transformation)

- Input - A User U provides a series of fingerprint images <f01 (x), f02 (x), ..., f0T(x)> as input B. A conventional fingerprint scanner or high-quality PC camera can be deployed for acquiring those images.
- Key Split - GΣ (1_) outputs an RSA public-private key pair, <e,N> and <d,N>

  As for the private exponent, an t-bit integer d1 is chosen at random to be relatively prime to φ(N) and d2 is computed for a large integer k as follows:

  d2 = dd1-1 mod φ(N) + kφ(N).
- Image Processing- A series of input images are combined with a random phase array to create two output arrays, Hs(u) and c0(x), where Hs(u) = e−iϕA0(u)eiϕR(u) and c0(x) = FT−1{A0(u) · |H0(u)| · Hs(u)}
- Encoding - Given the partial key d1, the central t/2× t/2 portion of c0(x) must be extracted and binarized for majority-encoding d1. A complex element a + bi at position (x, y) of the t/2× t/2 portion of c0(x) will be fragmented in the way that a will appear at (x, y) and b at (x + t/2, y) in the t × t/2 binarized template.

  Now the binarized template, bt, contains t22 real values that can be binarized with respect to 0.0, i.e., set as 1 if they are equal to or greater than 0.0, and otherwise 0.
- Possession - Finally, the user's possession P is defined as BT = {Hs(u), L} and PT = {d2, N}.

2) Signature Generation (T2 Transformation)

- Input - A User U provides a series of fingerprint images <f11 (x), f12 (x), ..., f1T(x)> as input B along with his or her possession <BT, PT >, say <Hs(u), L, d2, N>, in 2D bar codes that are readable by a PC camera.
- Image Processing - A series of input images are combined with Hs(u) to create a new output array, c1(x) where c0(x) = FT−1{A1(u) · |H1(u)| · Hs(u)}.
- Majority Decoding - Given the lookup table L, the central t/2× t/2 Portion of c1(x) must be extracted and binarized for majority-decoding d1. A method to obtain the new binarized template, bt', is exactly the same to that of key generation process. From bt1 and L, we can compose a new table L1 which may majority-decode d1 in the way that a majority bit in each column is derived to each location in d1.
- Signature Generation - Given an arbitrary message M, S raises it to the power of d1 and subsequently the result to the power of d2 for obtaining the corresponding signature Md ≡ (Md1)d2 (mod N). This is obvious because d ≡ d1d2 ≡ d1{dd1- 1 mod φ(N) + kφ(N)} (mod φ(N)).

3) BioGamal Algorithm (DNA Algorithm)

The combination of two algorithms i.e. DNA encryption/decryption algorithm and elgamal encryption/decryption algorithm is being performed by BioGamal Algorithm process.

a) DNA Algorithm

In the first level, the DNA Cryptography is being used to encrypt the hash value of the given data. The binary coding is being encoded by two states, preferably 0 or 1 along with a combination of 0 and 1 as shown in Table 1.

TABLE I. DNA DIGITAL CODING

BINARY VALUE	DNA DIGITAL CODING
00	A (ADENINE)
01	T (THYMINE)
10	G (GUANINE)
11	C (CYTOSINE)

Notations: M= plaintext and C1 ′ =Encrypted Cipher-text by DNA

b) DNA Encryption Algorithm

```
Cipher (byte M ′, byte C1')
State =M';
begin {
        convert ASCII code(state);
        convert binarycode(state);
        pairing(state);
        DNA digital coding(state);
        DNA sequencing(state);
      C1 ′ = DNA sequencing(state);
 end
}
```

c) DNA Decryption Algorithm

```
Decipher (byte C1 ′, byte M')
State = C1
begin {
    DNA_op.sequencing(state);
    [//op.sequencing applies for opposite DNA sequence]
    DNA_digital.decoding(state);
    Convert binarycode(state);
    Convert ASCII(state);
```

M′ = convert byte(state);

end

}

C. Elliptic Curve Cryptography

1) Elliptic Curve

Informally, an Elliptic Curve is a type of cubic curve determined by an equation of the form

$$Y^2 = x^3 + ax + b \quad (1)$$

where a and b are real numbers.

The elliptic curve also requires that the curve be non-singular.

Commutatively, this means that the graph has no thresholds, self-intersections or isolated points. Analytically, thus involves calculation of the discriminant

$$D = 4a^3 + 27b^2 \neq 0 \quad (2)$$

The curve is expected to be non-singular if and only if the discriminant is not equal to zero. Hence it is unsafe to use singular curves for cryptography as they are very easy to interpret, and for this reason, non-singular curves are not taken generally for data encryption.

a) Elliptic Curves over $F2^m$

The binary finite field executes the elements of $GF(2^m)$ can be depicted by m-bit binary code words. Therefore, it implies that a finite field of $GF(2^m)$ has characteristic 2. The equation of the elliptic curve on a binary field $F2^m$ is

$$Y^2 + xy = x^3 + ax^2 + b \quad (3)$$

b) Arithmetic in $GF(2^m)$

The brief introduction of the arithmetic operations to implement ECC point multiplication over binary the binary polynomial fields $GF(2^m)$, whose operation includes modular addition, subtraction, multiplication, squaring, division and inverse; where the operands are polynomials with coefficients of either 0 or 1. Thus we use the polynomial basis representation where $a(x) \in GF(2^m)$ in canonical form is written as

$$a(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_2x^2 + a_1x + a0 \quad (3)$$

2) Digital Signature by ECC

- Input – Domain parameters = (a, b, P, h, n) private key g, pixel values m.
- Output – Signature (s1, s2)
- Algorithm –

1. Select k ∈ R [1, n-1]
2. Compute kP = (x1, y1) and convert x1 to an integer x1 bar.
3. Compute s1 = x1 mod n. If s1 = 0 then go to step 1.
4. Compute d = SHA-1 (m).
5. Compute s2 = k -1(d + g s1) mod n. If s2 = 0 then go to step 1.
6. Return (s1, s2).

D. Image Authentication

1) Invariants of DCT Coefficients before and after JPEG Compression

A duplet of the DCT coefficients is located in the same position of any two non-overlapping image blocks maintains the constant relationship before and after JPEG quantization as follows:

1. if AFp,q(v) > 0, then AFp,q(v) ~ 0;
2. if AFp,q(V) < 0, then AFp,q(v) <~ 0;
3. if AFp,q(V) = 0, then A~'p,q(V) = 0;

2) Watermark Generating

The major content which should be related to Watermark message for the image and which must also survive the JPEG compression has the algorithm where the integer wavelet transformation proposed by Calderbank and Daubechies is being adopted.

3) Watermark Embedding:

The procedure is being as follows... Suppose B is taken as an image to be watermarked, then it is divided into some sub-images. Sizes of the sub-images are being determined by the watermark bit lengths. Repeatedly, the watermark will then be embedded into the sub-images and for each sub-image B(i), it is being divided into non-overlapping 8 x 8 blocks; where the DCT coefficients of each block are then quantized with the table of quantization at quality factor of 0.5 of JPEG compression.

4) Watermark Extracting and Integrity Authentication of the Image:

This approach can not only authenticate the original image but also the compressed JPEG image, keeping in mind that it can be recovered to the uncompressed one. This scheme is a replica of the insertion process.

5) Analysis of the Algorithm Performance:

After all this steps the finals step is to analyze the whole algorithm in many steps which includes –

1. The first step is based on the algorithm which is based on the knowledge of the authentication mechanism with the absence of the private key which reaches the extent of cryptography.

2. The second step depicts the order relationship between DCT coefficients in JPEG compression and marks the values of coefficient at 0.5 quality factor, for the survival of the compression to 0.5 or even less than 0.5.
3. It is followed by the above step where it is followed by the usage of coefficients in sub-band H3H3 followed with a 3-scale wavelet decomposition that reflects the edge of an image with the watermark that is being generated keeping in count of the content dependent and toleration of the compression.
4. The last step is a combination of image features that enhances the security of watermarking algorithm.

E. Lightweight SCDSA

1) Shortened Complex Digital Signature Algorithm (SCDSA):

This algorithm uses complex numbers that has CDLP which is used for designing SCDSA that makes it more secured as compared to DSA (Digital Signature Algorithm) schemes, DLP (Discrete Logarithm Problem), IFP (Integer Factorization Problem). SHA-1 key is used to secure hash function to fix the size of r to 160 bits.

- Basic Parameters, Key Generation, Signature Process and Verification Process
- Pseudo Code I – Signature Process on m
- Pseudo Code II – Verification Process on received message
- Proof I – Correctness Proof

2) Multi-option Parameter Selection (MPS):

This operation achieves the flexibility of the signatures that are generated using private key which the signer uses for a selected program which is also used for parameter calculation which can also be verified by the receiver by using the public key provided by the sender.

F. On Paper Digital Signature

1) OPDS Creation Procedure at Sender:

The sender verifies the authentication of the document containing QR code to check the content integrity, with two modes of verifier authentication mechanism: registered mobile phone number and registered E-mail ID.

2) OPDS Verification Procedure at Receiver:

The receiver verifies the authentication just as the sender with the particular verification method used at sender's end for the authentication of the document to check the content integrity.

.

IV. RESULT

After analysis it is observed, the ADS system achieves high system security that improves the efficiency and can also effectively achieve authentication of the collaborators' which makes it an ideal e-Government authentication mechanism.

On the other hand, the biometric system comprises of biometric encryption, fingerprint verification and bar-code technology is used to generate a digital signature to check the integrity which is highly efficient. The BioGamal/DNA algorithm designed to secure the data files uses biological sequencing to generate cipher text.

ECC modifications are used for the authentication of image to verify the sensitive content along with the authentication of watermarks. The watermarking algorithm are used to tolerate compression and for detecting and locate tampering simultaneously with digital signature and semi-fragile watermark.

TABLE II. RESULTS OBTAINED BY DIFFERENT METHODS

Keywords	Result
Arbitration Digital Signature	Hybrid Cryptosystem based on ADS System can access collaborators' authentication.
Biometrics	Biometric based digital signature generation system is highly efficient to check integrity of data and user authentication purpose.
Elliptic Curve Cryptography (ECC)	Applicable for image authentication for verification method while being sensitive to content-changing modifications with an embedded digital signature.
Image Authentication	Data will be analysed first for authenticated watermarks, then an image authentication along with semi-fragile watermark is proposed to locate and detect, tampering simultaneously.
Lightweight SCDSA	It is applied to compare the counter parts in terms of total time consumption, verification time and communication cost for signature-based messaging with authenticated verifications along with the probability of compromising intermediate devices which can be used in smart appliances.
On Paper Digital Signature (OPDS)	This is used in securing the privacy of an on-paper information to create a password using characters from a special signature, which is an end-to-end encryption.

The Lightweight SCDSA can be used for signature and verification process which are revealed by subverting devices and the probability of compromising intermediate devices.

And it is also used to secure the privacy of on paper information by choosing some characters of a special signature to create a password which must be known by both sender and receiver to access the information.

V. CONCLUSION

Studying and reviewing all the above-mentioned topics, we can say that Digital Signatures are the future of one's personal security. With all the methods and various types of Digital

Signatures we might implement these systems in any smart appliances, main frame systems and server securities. The development of authentication and verification will be upgraded to the next level, thus allowing every single person to have safe and protected information with utmost security.

The future e-Government authentication mechanism will be highly dependent on the end-to-end encryption. Not only that, even the signature passwords along with security biometrics and image authentication encrypted with DNA algorithm will all be secured using the hybrid arbitration cryptosystem which can be a combination of ECC, BioGamal Algorithm, Lightweight SCDSA and MPS.

Every single person will have the authority of their own security credentials along with IoT (Internet of Things). But as we know, everything has its advantages and disadvantages so there are and will be chances in the future for this system to have its own drawbacks. The drawbacks can be system failure, unable to retrieve lost information due to lack of system space and changing of one's personal security if necessary, in emergency cases or health issues.

The measure of these issues can be taken in the future with huge storage facilities like the mainframe systems consisting of trillion terabytes (TB) and back-up system along with safety measures to retrieve if any data is lost or if any authorization needs to be changed in case of emergencies or any alternative measures needs to be taken for authenticated signature and verification change.

REFERENCES

[1] Songnan Zhao, Ran Wei, and Zhimin Yang, "Research and Application of Arbitration Digital Signature Scheme Based on Hybrid Cryptosystem in e-Government," Pervasive Computing and the Networked World. ICPCA/SWS 2013. Lecture Notes in Computer Science, vol 8351. Pp. 827-833, Springer International Publishing Switzerland 2014. https://doi.org/10.1007/978-3-319-09265-2_85.

[2] Taekyoung Kwon, Jae-il Lee, "Practical Digital Signature Generation Using Biometrics, " Computational Science and Its Applications – ICCSA 2004. ICCSA 2004. Lecture Notes in Computer Science, vol 3043. Pp. 728-737, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24707-4_85.

[3] Rashmi Kasodhan; Neetesh Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm, " 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 27-29 March 2019, Erode, India. DOI: 10.1109/ICCMC.2019.8819710.

[4] T.N. Shankar, G. Sahoo, and S. Niranjan, "Digital Signature of an Image by Elliptic Curve Cryptosystem, " Advances in Computer Science and Information Technology. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 86. Pp. 337-346. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27317-9_35.

[5] Hong-Bin Zhang, Cheng Yang, Xiao-Mei Quan, "Image authentication based on digital signature and semi-fragile watermarking, " J. Comput. Sci. & Technol. Vol. 19, Pp. 752–759 (2004). https://doi.org/10.1007/BF02973435.

[6] Muhammad Arif Mughal, Xiong Luo, Ata Ullah, Subhan Ullah, Zahid Mahmooda "Lightweight Digital Signature Based Security Scheme for Human-Centered Internet of Things, " Special Section On Human-Centered Smart Systems And Technologies, June 29, 2018. Vol. 6. Pp. 31630-31643. DOI : 10.1109/ACCESS.2018.2844406.

[7] Sajan Ambadiyil, V. B. Vibhath and V. P. Mahadevan Pillai, "On Paper Digital Signature (OPDS), " Advances in Signal Processing and Intelligent Recognition Systems. Advances in Intelligent Systems and Computing, vol 425. Pp. 547-558. Springer, Cham. https://doi.org/10.1007/978-3-319-28658-7_46.

[8] Ralph C. Merkle, "A Certified Digital Signature, " Advances in Cryptology — CRYPTO' 89 Proceedings. CRYPTO 1989. Lecture Notes in Computer Science, vol 435. Pp. 218-238. Springer, New York, NY. https://doi.org/10.1007/0-387-34805-0_21.

[9] Selim G. Aki, "Digital signatures: A tutorial survey, " Computer, Volume: 16, Issue: 2, Pp. 15 – 24, Feb. 1983. DOI: 10.1109/MC.1983.1654294.

[10] Ananthi Sheshasaayee, B.Anandapriya, "Digital signatures security using cryptography for industrial applications, " 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 21-23 Feb. 2017, Bengaluru, India. DOI: 10.1109/ICIMIA.2017.7975640.