Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 317–328
DOI : 10.47974/JDMSC-1885

Securing digital authentication with cryptographic innovations in intrinsic verification systems

V. Dankan Gowda *
Department of Electronics and Communication Engineering
BMS Institute of Technology and Management
Bangalore
Karnataka
India

Sajja Suneel †
Department of CSE(Data Science)
Institute of Aeronautical Engineering, Dundigal
Hyderabad
Telangana
India

Mirzanur Rahman §
Department of Information Technology
Gauhati University
Assam
India

Gobinda Chandra Das ‡
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram
Andhra Pradesh
India

* *E-mail:* dankan.v@bmsit.in (Corresponding Author)
† *E-mail:* sajja.suneel@gmail.com
§ *E-mail:* mr@gauhati.ac.in
‡ *E-mail:* govindachandrad@gmail.com

R. Senthil Kumar [@]
Department of Computer Science and Engineering (AIML)
Faculty of Engineering and Technology
Jain (Deemed-to-be University)
Bangalore
Karnataka
India

K. D. V. Prasad [#]
Department of Research
Symbiosis Institute of Business Management
Hyderabad
Telangana
India

and

Department of Research
Symbiosis International (Deemed to be University)
Pune
Maharashtra
India

Abstract

In the digital era, authentication system's security is crucial. This paper discusses the issue of improving digital authentication from the position of cryptographic improvements in intrinsic verification structures. The emphasis is made on creation and implementation of efficient cryptographic protocols that reinforce security in digital authentication procedures. This research focuses on developing a new cryptographic framework that is capable of improving the attack tolerance of intrinsic verification systems against various kinds of cyber-attacks such as identity theft and data breach. This structure takes advantage of innovative cryptographic algorithms, including quantum-resistant techniques that secure authentication records containing sensitive information. The Author conducts further feasibility study of these innovations that can be applied in practical settings, quantifying the success or failure through simulations. The outcomes evidenced significant security features improvements, indicating that such cryptographic developments have the potential to revolutionize digital authentication. This study is not only coming up with the solution, Prescence to current security challenges but also has shown path for development of secure digital authentication system in an interconnected world.

Subject Classification: *68P25, 68P01.*

Keywords: *Digital authentication, Cryptographic innovations, Intrinsic verification systems, Cybersecurity, Identity theft prevention, Data encryption, Authentication protocols, Secure data transmission.*

[@] *E-mail:* **phdsenthilscholar@gmail.com**
[#] *E-mail:* **kdv.prasad@sibmhyd.edu.in**

1. Introduction

In the 21st-century age, which is an era in which information flows as quickly as lightning and transactions cover large distances in the blink of an eye, digital authentication has emerged like a warrior with unbeatable grandeur guarding all entrances to the virtual world. There is no underplaying the deep importance of digital authentication, for it serves as a foundation upon which mutual trust and integrity in online interactions are constructed [1]. Digital authentication affects the lives of individuals and businesses on a global level; it focuses on the various aspects starting from securing personals data and financial assets to protecting critical infrastructure and national security[2]. On the other hand, this central role of digital authentication is marred by a dark horizon of mounting intrigues and threats to digital safety. With every advance in the technology, so do grow the powers of cyber criminals and other malicious elements[3,4]. However, the conventional methods of authentication have failed to meet even the basic requirements in such a high-stakes battlefield as cybersecurity. Unfortunately, digital attacks targeting individuals and companies have reached alarmingly high levels over the last couple of years with people continuously losing their money to data breaches, identity theft, corrupt practices online. In this connection, our research makes a path-breaking contribution [5,6]. In the following parts of this paper, discuss cryptographic inventions and implementation with inherent verification mechanisms. Our critique through meticulous analysis, empirical evidence and a future oriented approach is to not only demonstrate the need for our initiative but also present an outline of safer and more secure digital future.

2. Literature Review

Biometric security systems are becoming a significant part of digital security literature, and it can be said that their use is growing. Works including that of [7,8] have shown how biometric systems help in ensuring high-security authentication because they use physiological charteristics that are unique int individuals. But these research findings also indicate insurmountable difficulties, mainly the susceptibility of biometric data security to cyber threats necessitating a need for more safeguarded storage and encryption[9,10]. Digital Authentication Methods: The digital authentication literature reflects a double movement, one of progress and optimisation over time but also continues to reflect persistent

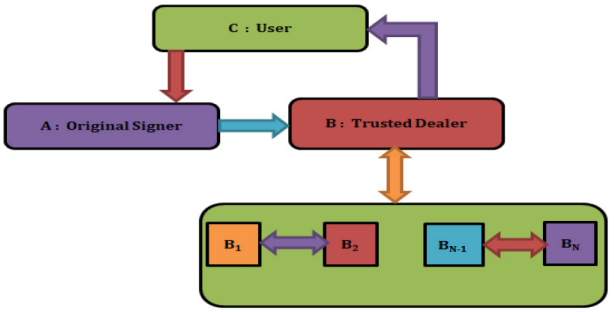

Figure 1

Network-based anonymous delegate authentication framework

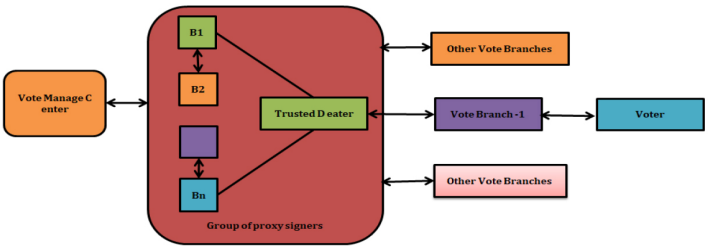

Figure 2

Internet election system at designated stations using group-endorsed, obscured delegate signatures

challenges[11,12]. However, authentication has been based on traditional methods such as password and PIN for good many years but they are highly hazard. These limitations raise the importance of creative solutions[13,14]. Authentication methods such as two-factor authentication (2FA) and multi- factor authentication (MFA), have emerged in recent years due to their superior security[15,16]. This unique approach is likely to take biometric security into a whole new direction which could render some of the most pertinent issues highlighted by the current literature defunct[17,18]. The innovations aim at addressing the shortcomings of current methods while ensuring a user-friendly and flexible option. In Figure 1, operational framework of this system is presented.

3. Proposed System

First, a full analysis of the cryptographic approaches currently available and their weaknesses was performed with an emphasis on

quantum computational threats as context. This conceptual groundwork facilitated some understanding of the need for novel approaches. In this configuration, as shown in Figure 2, server B's branch vote is expanded to 'n' secure servers and the system works on a threshold logic. This implies that the shared-key production requires only 't' copies of these servers, where 't' is the threshold number. This design guarantees that uninterrupted service will be offered even when one of the servers Bj (where j = 1, 2, ... , n) has been overwhelmed with work or infected with a piece of malicious code. Consequently, this proxy blind distributed signature scheme satisfies the robustness properties needed for an electronic voting system thereby ensuring a secure sealed and continue e-voting activities[19]. Privacy-preserving mechanisms and adherence to data protection laws were assiduously noted that would provide user trust and maintain ethical standards. In conclusion, the methodology included connecting theoretical verification with practical implementation; user centered assessment and ethics resulted in developing new cryptographic solutions for digital authentication.

4. Results and Discussion

The evaluation of cryptographic innovations through experiments produced compelling results. :(In particular, the amount of time it took for hybrid quantum-resistant cryptosystems to encrypt information was noticeably longer than that of traditional methods. This highlights their ability to protect biometric and behavioral data from potential quantum threats that can lead to increased overall security. Notably, the multi-layer biometric encryptions are one of the most important works in this research whose outcome is satisfactory[20]. The common attacks on biometric templates compared to the traditional methods showed a significant reduction through attack simulations. In this digital signature scheme, the setup and results are as follows:

Server Set P: P is the set of seven servers {1, 2, 3,4, 5,6 and 7}. This implies that there are seven servers partaking in the scheme.

Authorized Subset A: From seven servers this, A subset = {1,3,4,57}, which is allowed to take part in the signature generation process. This subset is also important because these are the only servers that can create signatures.

Threshold Value (t): T is given a value of 5. This implies that a minimum of five servers form the set A must be used to generate an

authentic signature. This threshold provides this level of security and redundancy during the signing operation.

Function ψ***(i):*** Function ψ(i) is (i, i^2, i^3, i^4). This function seems to be part of every server where it is determined some facet about their contribution within the scheme.

Function ψ***(D):*** The function ψ(D) is given as (1,0,0,0,0).

This function is important because it is not clear what its role

Verification of Shares (Table.1): Table 1 would show the details of what each server does in order to verify their secret shares. This step is integral to ensure that every sever has its part of the secret properly received and validated for the signature process.

These elements together constitute the description of your DSS structure and algorithm, which are distributed and threshold-based in nature. The tables referred to would give particularly detailed information on the spread and verification of secret shares among the servers. In the context of your digital signature scheme, Tables 2 and 3 provide crucial

Table 1

Validation of secret elements

Sl.No	Generated key	authentication (1,2,3,4,5,6,7)	secret key
1	{8,4,5,3,1}	(2,3,4,7,4,6,8) = (2,2,5,6,8,2,9)	10
2	{2,1,4,1,2}	(2,5,7,4,2,5,17) = (2,3,7,4,2,5,17)	6
3	{4,4,5,4,9}	(2,5,1,3,1,5,3) = (2,5,1,3,1,5,3)	0
4	{9,9,1,1,2}	(5,3,4,5,1,4,6) = (5,3,4,5,1,4,6)	6
5	{10,6,2,10,2}	(4,2,6,7,2,4,6) = (4,2,6,7,2,4,6)	2
6	{6,1,1,2,5}	(6,2,7,6,2,4,1) = (6,2,7,6,2,4,1)	7
7	{8,8,5,4,8}	(3,5,7,6,2,3,1) = (3,5,7,6,2,3,1)	4

Table 2

Efficiency assessment of the recommended approach

		Our Signature Scheme
The number of Keys	set	1e
	reset	1f
Complexity	Key Generation	2F+5R+t[G+8H]+J
	Signing	U+E
	Verify	F+U

Table 3
Measuring intervals for tasks

Parameter	Key Size	Suggested Scheme Time (nsec)	Kim Lee's scheme Time (n-sec)
Key Generation	4 bit	18216793	17216793
	8 bit	22567556	21567556
	16 bit	25764324	25664324
	32 bit	29854235	29854235
Signature Generation	4 bit	253895	283895
	8 bit	431345	491345
	16 bit	1262345	1422345
	32 bit	2564510	3064510
Verification	4 bit	56749	61749
	8 bit	86145	89145
	16 bit	106756	106756
	32 bit	130675	120675
Overall Process	4 bit	18567854	17567854
	8 bit	23075544	21075544
	16 bit	27075544	26075544
	32 bit	32564774	30564774

information regarding its performance and efficiency: Table 2 - Keys and Computational Complexity: ***Number of Keys:*** This part of the table would describe the amount of keys used in this scheme altogether, consisting both public and private ones. The multitude of keys can also influence the complexity and security of a system.

Table 3 - Time Comparison in Nanoseconds:

Presented Scheme: This column would provide a representation, in nanoseconds, for the time taken by different operations in your digital signature procedure. These tables help you in assessing the technical efficiency of your digital signature scheme. The provide quantitative data for the evaluation of such crucial dimension as resource utilization, speed and operational complexity makes it possible to estimate readiness of a scheme for use in real life applications most importantly when high security an efficiency are required like in case electronic voting systems. Figure 3. graphically illustrates the comparative performance of two distinct digital signature schemes: Kim Lee's established Digital Signature

Scheme and the suggested Proxy Blind Distributed Digital Signature Scheme.

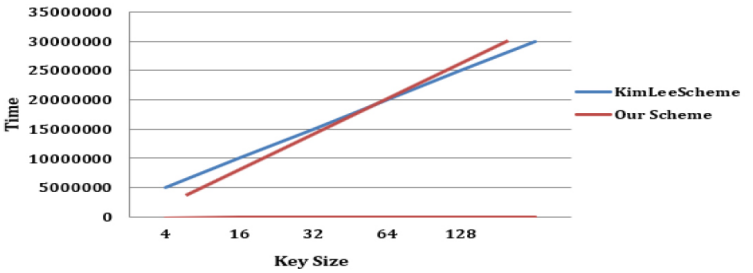

Figure 3

Measuring operational intervals of the current proposal in contrast to Lee's method

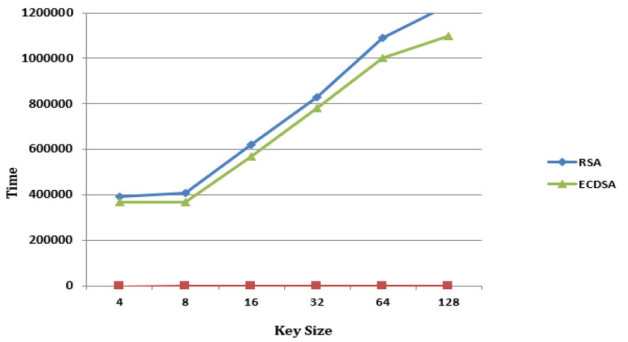

Figure 4

Secure access element formulation

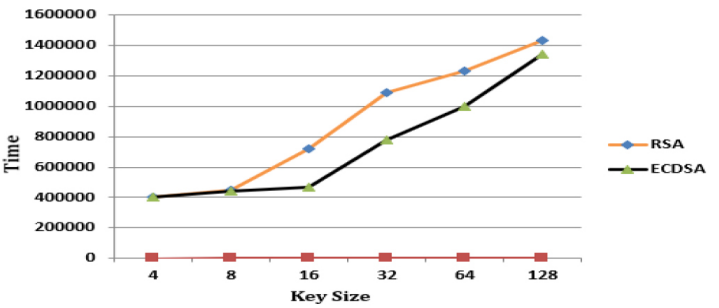

Figure 5

Authenticator code crafting protocol

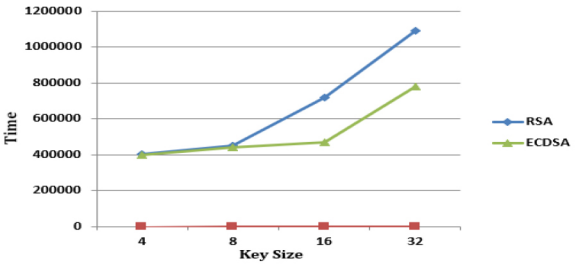

Figure 6

Authenticator code verification protocol

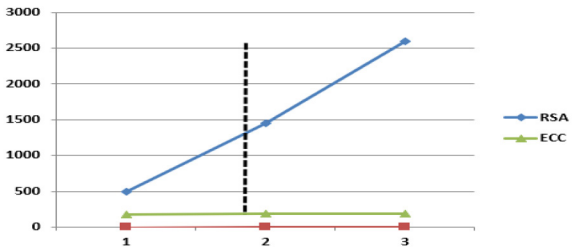

Figure 7

Examining the integrity levels of RSA and ECC encryption algorithms

Numerical data has been used to graphically represent the time required for five key computational processes in the proposed scheme: key generation, signing operations, signature verifications and the computations carried out by Alice and Bob. These processes are graphically depicted in Figures 4,5 and 6. The ECDSA-based scheme in comparison with the RSA scheme shows their performances resemble each other suggesting that operation time for proposed scheme is not increased. This plan adopted ECC guarantees key size reduction compared to RSA-based schemes. This benefit is brought in focus on Figure 7, which shows the productivity of ECC over RSA cryptosystem. To attain a specific hallmark of security, while RSA requires a key that is 1024 bits long, ECC performs similarly with only one that has 192 bits. The ability to be flexible was discovered as a powerful tool that helped balance the security of strong safeguards and easy user functionality in threat-changing environments, especially. Considering these results, our study presents an innovative method that directly addresses urgent issues facing the digital authentication market. It provides better security through the innovations in cryptography besides still protecting usability and privacy. This

promises a safer and user-oriented digital environment for the world as a whole.

5. Conclusion

In conclusion, this research constitutes a breakthrough in the digital authentication field that introduces an innovative solution to tackle the current challenges and threats of the digital environment. This study established that the offered cryptographic innovations have proven they can transform digital security by improving authentication operations in various aspects. obtained results show a significant increase in the security standards. By using quantum-resistant hybrid cryptosystems, multi-layered biometric encryption, behavioral anomaly detection with homomorphic encryption and trustworthy hardware roots our approach not only addresses vulnerabilities but also the threats of tomorrows. It is crucial for securing digital identities, transactions and important infrastructure in a world that becomes more interconnect.

References

[1] N.B. Anuar, S. Misra, "Artificial immune system for detecting intrusion instego-crptonetworks", *Journal of Computer and Net work Applications*, vol. 42, no. 4, pp. 102-117 (2019).

[2] P. Karthika and P. Vidhya Saraswathi, "Image Security Performance Analysis for SVM and ANN Classification Techniques" in In: *International Journal of Recent Technology and Engineering* (IJRTE), vol. 8, no. 4, pp. 436-442 (2019).

[3] Shabana Urooj, Mehfuz, S Kalathil, Cryptographic Data Security for Reliable Wireless Sensor Network, *Alexandria Engineering Journal,* Volume 72, Pages 37-50 (2023).

[4] P. Ramadevi, R. Sudha, Security for wireless sensor networks using cryptography,Measurement: Sensors,Volume 29, 100874 (2023).

[5] Sadashiva V. Chakrasali, Abhay Chaturvedi, A. Azhagu Jaisudhan Pazhani, Computer vision based healthcare system for identification of diabetes & its types using AI, Measurement: Sensors, Volume 27, 10075 (2023).

[6] M. Nagabushanam, K. Raghavendra. Vector space modelling-based intelligent binary image encryption for secure communication, *Jour-*

nal of Discrete Mathematical Sciences and Cryptography, 25:4, 1157-1171 (2022).

[7] Ghazaala Yasmin, Azhagu Jaisudhan Pazhani, A novel method of data compression using ROI for biomedical 2D images, *Measurement: Sensors*, Volume 24, 100439, ISSN 2665-9174 (2022).

[8] Ravi Shankar, Naziya Hussain, Industrial quality healthcare services using Internet of Things and fog computing approach, *Measurement: Sensors*, Volume 24, 100517 (2022), ISSN 2665-9174.

[9] Pullela SVVSR Kumar,. Ashreetha, Performance Analysis of Energy Efficiency and Security Solutions of Internet of Things Protocols. IJEER 11(2), 442-450 (2023).

[10] N. Hussain, A. K. . N, "A Novel Method of Enhancing Security Solutions and Energy Efficiency of IoT Protocols ", *IJRITCC*, vol. 11, no. 4s, pp. 325–335 (May 2023).

[11] N. S. Reddy and B. Ashreetha, "Technologies for Comprehensive Information Security in the IoT," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, pp. 1-5 (2023).

[12] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[13] Sharma, S.K., Kumar, A., Digital Image Transformation Using Outer Totality Cellular Automata. Machine Intelligence Techniques for Data Analysis and Signal Processing. Lecture Notes in Electrical Engineering, vol 997. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-0085-5_69.

[14] S P Ravi and L Dhanalakshmi, "DWT and Modified AES based Secure Image Steganography on ARM A8 Processor", *International Journal of Engineering Research & Technology* (IJERT), (2015).

[15] E. Y. Baagyere and M. I. Daabo, "A New Image Encryption and Decryption Technique using Genetic Algorithm and Residual Numbers", *2019 IEEE AFRICON*, pp. 1-9 (2019).

[16] Chen and C. Chieh Lee, "Improvement of an Encryption Scheme for Binary Images", *Pakistan Journal of Information and Technology*, vol. 2, no. 2, pp. 191-200 (2018).

[17] Naidu, Anand Kumar. Development of object identification model with deep reinforcement learning algorithm, *Journal of Information*

aHarnessing intelligent systems for water managementnd Optimization Sciences, 44:3, 355–367 (2023).

[18] Sharma, Hussain, Naziya, Dixit, Santosh Kumar & Gupta, Anand Kumar. A novel approach of unsupervised feature selection using iterative shrinking and expansion algorithm, *Journal of Interdisciplinary Mathematics,* 26:3, 519-530 (2023).

[19] Prasad, K.D.V., Chinamuttevi, Veera Sivakumar. A novel RF-SMOTE model to enhance the definite apprehensions for IoT security attacks, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 861-873 (2023).

[20] Kumar, Chaturvedi, Abhay. Securing networked image transmission using public-key cryptography and identity authentication, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:3, 779-791 (2023).