Using Artificial Intelligence (AI) and Internet of Things (IoT) for Improving Network Security by Hybrid Cryptography Approach

Sumathi M S
BMS Institute of Technology and Management

J, Shruthi
BMS Institute of Technology and Management

Jain, Vipin
Teerthanker Mahaveer University

G Kalyan Kumar
Rajalakshmi Institute of Technology

他

https://doi.org/10.5109/6793674

出版情報：Evergreen. 10 (2), pp.1133-1139, 2023-06. 九州大学グリーンテクノロジー研究教育センター
バージョン：

Using Artificial Intelligence (AI) and Internet of Things (IoT) for Improving Network Security by Hybrid Cryptography Approach

Sumathi M S[1,*], Shruthi J[2], Vipin Jain[3], G Kalyan Kumar[4], Zarrarahmed Z Khan[5]

[1, 2]BMS Institute of Technology and Management, Bangalore, India

[3]Teerthanker Mahaveer University, Mordabad, Uttar Pradesh, India

[4]Rajalakshmi Institute of Technology, Chennai, India.

[5]Anjuman I Islam Kalsekar Technical Campus, Mumbai University, India.

*Author to whom correspondence should be addressed:

E-mail: sumathi.m@bmsit.in

(Received February 1, 2022; Revised May 14, 2023; accepted May 14, 2023).

Abstract: Cryptography is defined as the analysis of encryption or secretive writing of information with the use of mathematical & logical concepts in order to prevent data from being compromised. Because of the growing security issues around Internet of Things (IoT) & artificial intelligence (AI) based applications, this method has gained in significance in computer technologies for banking & healthcare systems, transportation, as well as other implementations. Although each cryptographic strategy is designed to have its own unique strength, the application of a single cryptographic strategy into a systems has certain drawbacks, as will be discussed below. For example, the symmetric key encryption approach is a cost-effective way of protecting information that does not sacrifice security in the process. The distribution of the private key, on the other hand, is a significant issue. The asymmetrical method, on either side, overcomes the problem of private key transmission; nevertheless, the independent approach is slower and uses more computer resources as comparing to symmetric encryption. While a hash function, on the other hand, produces a distinctive & fixed-length signatures for a communication in order to ensure information security, the technique is just a one-way function that is not possible to reverse. As an option to addressing the security flaws of individual cryptographic schemes, the inclusion of many cryptographic schemes, also known as the hybridization approach, is being suggested, which has the advantage of increasing the efficiency of information security while also discussing the problem of key transfer. Existing IoT & AI domains that have adopted hybrid methods have been recognized, and a study has been carried out as per classification of the domain under consideration. The security of the networks and the data sent over the network is a top priority for network providers or network operators. As a result, cryptographic methods are used to protect the data throughout the data exchange process and during different interactions. Traditional cryptographic methods, on either side, are well-known, because hackers are aware of the answer to the problem. As a result, a fresh type of cryptographic method is needed, one that increases the security & complexities of the data encryption while maintaining its simplicity. An innovative hybrid cryptographic approach for enhancing data security throughout networks transmission is presented in this article, and the consequences of its implementation and evaluation are discussed. Throughout a comparative performance study, the suggested cryptographic method was able to identify the most efficient & enhanced encrypted message.

Keywords: Artificial Intelligence (AI), Internet of Things (IOT), Cryptography, Encrypted, Security, Network, Information, Public and Private Key, Decode, Encode

1. Introduction

An encrypted message is a method of safeguarding data by transforming it (encoding it) into an incomprehensible format (for human vision). Only those with connectivity to the secret key are able to decrypt (or decode) the communication into plain text. Despite the fact that today's encryption techniques are virtually impregnable, encrypted communications may sometimes be broken via cryptanalysis, also known as code-breaking[1)]. As the Web

and other forms of digital communication become more popular, digital security has become more important. Cryptography protects e-mail conversations, credit card information, and corporate data. Because it is both effective and inexpensive, Fairly Decent Security is a well-known encryption method on the Internet. Cryptography systems are usually classified as synchronous, which use a single key that both the sender and the receiver have, or public-key, which use a pair of keys, a publicly known key and a secret key that only the message's recipient knows. There seem to be a plethora of applications available at the moment that enable sensitive and private information to be transmitted over an unsecured network. Essentially, most of the time, a user sends data from a reliable network to other safe network. The network between the source and destination hosts, however, remains unsecure[2]. As a consequence, the bulk of applications use cryptographic techniques to ensure data security & privacy.

The Internet of Things (IoT) and Artificial Intelligence (AI) are interested in connecting the unconnected. It relates to the rapidly growing web sensing devices and technologies that accomplish data recognition, reliable communication, and intelligence technologies. IoT & AI are the combination of multiple data sensing devices, such as radio frequency identification (RFID), wireless sensor networks (WSN), cloud - based services, global positioning system (GPS), or the Web, to form a massive network and allow data monitoring and assessment, which involves giving a full spectrum of services to individuals everywhere depending on application integration. This technology is quickly expanding beyond operations to include smart neighbourhoods, intelligent transportation, intelligent financial systems, and other applications[3]. To provide reliable and excellent service, however, security issues across the system, including remote access and installation, must be resolved[4]. Many significant vulnerabilities in System elements such as wireless sensor networks, radio frequency identification devices (RFID), cloud - based services, and Machine to Machine (M2M) technologies have been discovered, including man in the middle, replay attacks, spoofing, and impersonating threats. These security vulnerabilities have also been found in artificial intelligence technologies, namely in e-commerce, medical/healthcare, biometrics, multimedia information sharing, and information transmission systems. In the course of the attack, the malicious individual may enter genuine user information into a changed system, boot the computer with a bogus software application, and so on. Furthermore, the intruder may spy on other people or information sent over the network by devices, mimic the real communicating device, and disclose critical information to an unauthorised third party. The development of the aforementioned privacy and security issues requires extra attention; therefore, unique solutions to each of these difficulties should be provided. Because potential IoT infrastructure attacks may result in application lack of control, loss of service, and loss of user privacy, among other security issues[5]. The process of combining the characteristics of multiple algorithms in order to increase effectiveness and efficiency and address issues with current methods is referred to as hybrid cryptography.

2. A survey of hybrid cryptographic techniques

Security is an essential feature of instruction set because it ensures that precious resources are not changed, duplicated, or made accessible to unauthorized individuals. To protect versus unauthorised assault, each proposed framework needs a unique variety of security characteristics including such information security, consistency, identification, & accessibility, which vary depending on the kind and value of its assets[6]. To accomplish these security characteristics, many security methods have been established, most of which rely on cryptographic algorithms including such symmetric & asymmetric encryption, hashing algorithms, object identification, consensus method, and many others[7].

There are three types of cryptography algorithms: symmetric encryption, asymmetric encryption, & cryptographic output functions. The symmetric encryption technique encrypts and decrypts data using a single secret key. As it only uses one key, this method is very efficient in terms of performance and processing power. Although Data Encryption Standard (DES) & Advanced Encryption Standard (AES) are both well-known symmetric approaches, AES is more secure than DES. Similar symmetric approaches include 3DES, RC2, RC4, RC6, and Blowfish methods. Despite the fact that symmetric encryption is very efficient in regards of computing, it has a flaw in key transmission. The major problem with this method is that the secret key must be exchanged safely and discreetly with an authorised communicating entity in needed to execute symmetric encryption over public transmission.

In comparison, asymmetric key cryptography, also recognised as public key cryptography, necessitates use of 2 distinct keys to encode & decode information: a secret key that is only identified and should stay secret to its corresponding proprietor for decryption, as well as a public key that is recognised to all organisations on the public site[8]. In this approach, the public key is used for encryption information, while another key, which is kept private, is used to decode the information. Rivest, Shamir, & Adleman (RSA), Diffie Hellman Key Extraction (DHKE) based consensus method, Al Gamal, & Elliptic Curve Cryptography are common examples asymmetric key approaches (ECC). These approaches are used to guarantee the information secrecy, validity, & non-repudiability security characteristics. The drawback of the asymmetric method is its slowness; it is considerably slower as symmetric encrypt since the calculations are

more complicated, which meaning the information takes a bit longer to encode & decode.

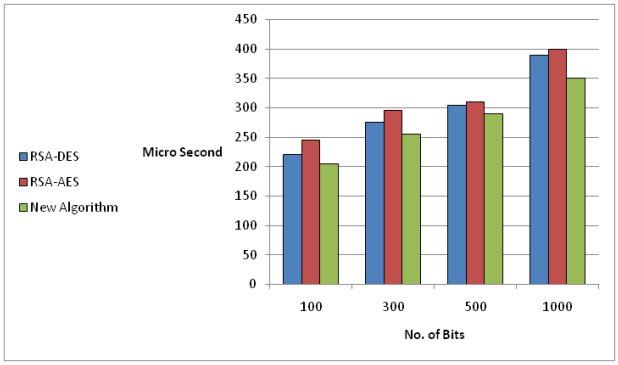

Fig. 1: Hybrid encryption/Decryption cryptographic technique

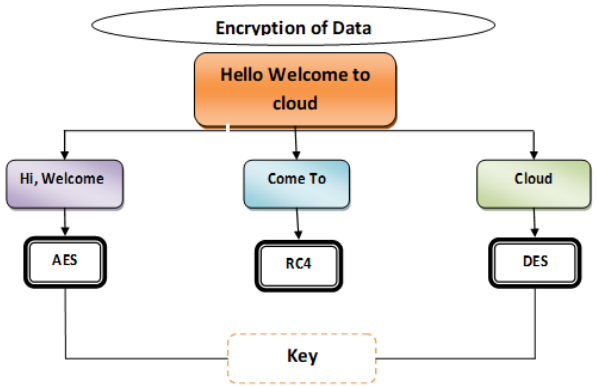

Fig. 2: Hybrid Cryptographic Techniques

However, asymmetric methods like DHKE & Al Gamal may be utilised to offer a safe mechanism for key negotiations in mainstream networks. Notwithstanding this, it is vulnerable to Man-In-The-Middle (MITM) attacks during the crucial transaction among those engaged in the procedure. In practise, a few cryptography methods are often coupled to increase security. Hybrid cryptography is the process of integrating the characteristics of just few techniques in order to improve reliability & effectiveness while overcoming the limitations of separate methods[9]. Combination is a noteworthy method that provides answers to key issues including such computing efficiency, effectiveness, or any other way to provide the highest sense of protection for a systems.

3. Cryptography's keys administration

It is possible to build the finest cryptosystem by using symmetric techniques since they are very quick in processing and safe in methods when compared to asymmetric techniques[10]. Moreover, one of the most difficult issues in cryptosystems is the dissemination of the private key via an insecure channel (Jain 2017). From this point on, this article will express viable data on how to combine corporation symmetric techniques with other techniques to create a new approach with high security in several areas. A cryptosystem key administration consists of many stages. The three most important are key creation, key distribution, & key cancellation. The transmission of the key is important because Eve is primarily interested in intercepting and catching the key. If a cryptosystem employs the toughest technique and generates the greatest key, but the key distribution lacks security, the total security of such cryptosystem is 0[11]. The Diffie Hellman technique pioneered key exchange protocol across insecure networks. In table 1. We show few of the security issues of key generation have been addressed in.

Key transmission that is secured	The keys should be properly secured throughout the distribution procedure to parties. They are the simplest method for Eve to get access to this information. Eve may target keys at a variety of stages, including key exchange, key upgrades, key cancellation, and so on[12].
Key organizational performance	For key administration procedures, many cryptosystems currently depend on centralised key verification agencies. All worth and importance of vital security is given to these powers here[13]. As a result, the efficiency & protection effectiveness of these certifying authority plays a significant role in ensuring protection to communication entities.
Information verification	The keys may be used to verify the identity of the communicating entity[14]. This functionality may be provided via public key cryptography.
The privacy of information	The primary function of cryptographic is to ensure data secrecy. Given the importance of keys in cryptosystem protection, they should satisfy this requirement.[15]

4. Hybrid cryptosystem using public keys techniques

Hybrid cryptosystems appear to be the best current way for a cryptosystem to offer the highest level of security feasible. They are termed hybrid techniques since they combine the protection & efficiency of symmetric cryptography with the power of asymmetric algorithms in safe key exchange, identification, and other applications. Although public key cryptosystems have a good strength, they also contain a number of flaws. In table 2. We show the list consists of some of these disadvantages

1	Asymmetric techniques are very susceptible to selected assaults. Because the secret key is public, this hack is successful.
2	Even though the databases that contains the values of the public - key is highly safe & only authorised users may change it, there is still a significant danger of Eve changing the database's contents[16].
3	A most common threat on a public key cryptosystem is a man-in-the-middle hack. The Interlocking Protocols has been suggested as a solution to this issue, however there

	are significant objections itself against efficiency and effectiveness.
4	Computational assaults are another concern in symmetric methods. Despite the notion that multiplying N is a virtually difficult computation, experts have shown the feasibility of this assault, particularly with the advancement of technology and the power of computer processors[17].
5	The pace of public key techniques is very slow. Although the use of symmetric methods has reduced this difficulty, it remains a concern in a symmetrical function.

Certification Administrators (CA) were developed as an alternative to open key exchange. However, there are still important problems for this approach, such as the words certificate, confidence, how to select the authorities on head of everybody, and how long that agency is trusted for.

5. Hybrid security technique in wsn and iot-related applications

WSNs are regarded as one of the advanced components in the implementation of IoT designs. Because of the distributed aspect of the data transmission, WSNs are susceptible to security threats. Because WSN nodes have limited energy and computing capacity, conventional security methods for these systems are challenging to apply. To address these concerns, several security techniques have been suggested to meet security criteria like as secrecy, identification, & consistency. Six publications were discovered that proposed a hybrid method to securing WSN-related IoT devices[18].

A hybrid security method in which two distinct approaches are used to secure 2 separating ciphertext. The first section of the information was protected using a mix of symmetric & asymmetric AESECC, whereas the second section was secured with XOR-DUAL RSA.

As an error checking, the MD5 hash algorithm was also used. Many performance measures were examined in this study, including ciphertext size, encryption/decryption time, time complexities, fuel, as well as the frequency of lost packets. Other study used a hybrid method, using cellular automata-based security mechanisms (CASM) for core administration and a current encrypted standards edition 1 (MES-1) symmetric method for information encryption in a wireless sensor network (WSN) systems[19]. The technique performed well against takeover attacks, low power transmission, receiver collisions, and other issues.

By combining asymmetric encryption & ECDH for key administration, the hybrid key organisational technique (HKO) was developed. The technique employed for information encrypted was not specified in this study, which assessed energy usage. MA-CBE is a light hybrid method that use a mix of 8-bit chaos blocks encrypting and Message Authentication Code (MAC)-based hashing. The study looked at compression ratios, given input quantity, information correlations, energy usage, and cost savings[20]. The findings demonstrated that this method provided considerable findings in terms of reliability & energy-efficiency in addressing the WSN's energy limitations. A certificateless hybrid signcryption method based on the randomized operator model that employs important & personal information. The method may be used to protect WSN communication systems for key administration & safe transit. Computational complexity & ciphertext length were assessed as performance indicators. A hybrid of hidden content aggregation (HCA) and a signatures method based on homomorphic encryption software. With an examination of the program's effectiveness, computing overhead, energy usage, and latency, the collaborative approach provided substantial consolidated findings[21].

6. Data Analysis

The current section enable in presenting the importance of using IoT in improving Network security by Hybrid cryptography approach.

Table 1: Quicker assessment

Quicker assessment	Frequency	Percent
Not at all important	15	9.9
Less important	4	2.6
Neutral	17	11.2
Important	49	32.2
Highly important	67	44.1
Total	152	100

Based on table 1, it is noted that 44.1% of the respondents mentioned that they are highly important stating that the IoT enable in quick assessment of issues related to cyber attacks, 32.2% mentioned that they are important.

Table 2: Better integration of application

Better integration of application	Frequency	Percent
Not at all important	13	8.6
Less important	14	9.2
Neutral	9	5.9
Important	55	36.2
Highly important	61	40.1
Total	152	100

Based on table 2, it is noted that 40.1% of the respondents mentioned that they are highly important stating that the IoT enable in better integration of application, 36.2% mentioned that they are important.

7. Artificial intelligence-related hybrid security technique in cloud computing, biometrics, or intelligent banking/e-commerce areas

The hybrid method has been used in many research, including cloud computing, biometrics, & smart banking/e-commerce networks. These categories are also a component of artificial intelligence applications, which eventually offer a complete variety of activities to individuals all over the world depending on the application connectivity. Only one article was identified that used the hybrid approach in cloud computing. A Lightweight Confidentiality Data Aggregation (LPDA) method that uses homomorphic Plaintext encryption, the Chinese Remaining portion Principle, and a single lane hash. Using differentially private methods, LPDA is highly secure & private information. Furthermore, the communications latency & computational complexity findings showed that LPDA is light in cloud computing improved AI [22] . In addition, two papers in the biometric-AI area have created the hybrid approach. A concept and development of an embedded platform for accurate and safe biometric authentication in which the information was secured using a hybrid encryption technique based on the Blowfish & RSA algorithms[23-26].

The suggested two-step verification provides the system with excellent security[27-30]. Face Information Fusion (FIF) is a hybrid data fusion method composed of three parts: the face algorithm, the RSA algorithm, and the FIF method. The suggested method might quickly identify individuals [31-32]. In four papers, the hybrid method in intelligent banking & e-commerce systems was described. The hybrid solution was split into two parts: safe identification and expense encryption[26]. This was accomplished via the use of multi-factor identification as well as the ECC method. When comparison to hybrid RSA, hybrid ECC used less bandwidth and took less time[27]. The use of hybrid AES & ECC encoding to secure information in electronic commerce, depending on an SMS-based paradigm. The method offered secure payments via SMS, which met all protection requirements. MD5 & RSA are used in a hybrid manner[28].

A five-phase verification method was used: User Id, User Passcode, User Different Id, Matching UID with customer Barcode, and an Once Time Password. The researcher said that RSA was implemented because it was quicker and had easy encrypting & authentication procedures. A very big number with two primary components (similar to RSA). To encrypt/decrypt information, DES symmetric encryption was used. The suggested approach clearly outperformed traditional HTTPS in terms of transaction performance

8. Results and Discussion

In the present work the authors have surveyed the usage of Artificial Intelligence (AI) and Internet of Things (IoT) for improving Network security by Hybrid cryptography approach. From the literature survey it has been perceived that cryptographic methods are used to protect the data throughout the data exchange process and during different interactions. Traditional cryptographic methods, on either side, are well-known, because hackers are aware of the answer to the problem. As a result, a fresh type of cryptographic method is needed, one that increases the security & complexities of the data encryption while maintaining its simplicity. An innovative hybrid cryptographic approach for enhancing data security throughout networks transmission is presented in this article, and the consequences of its implementation and evaluation are discussed. Throughout a comparative performance study, the suggested cryptographic method was able to identify the most efficient & enhanced encrypted message.

9. Conclusion

In this research we examine the survey of hybrid cryptographic techniques after that we briefly discussing the cryptography's keys administration. we study in this paper hybrid cryptosystem using public keys techniques. We also review in this study hybrid security technique in wsn and iot-related applications and last we examine the artificial intelligence-related hybrid security technique in cloud computing, biometrics, or intelligent banking/e-commerce areas.

References

1) V. Kapoor and R. Yadav, "A Hybrid Cryptography Technique for Improving Network Security", International Journal of Computer Applications, vol. 141, no. 11, pp. 25-30, 2016. Available: 10.5120/ijca2016909863.
2) "Enhancing Data Security Using Elliptic Curve Cryptography in Cloud Computing", International Journal of Science and Research (IJSR), vol. 5, no. 7, pp. 1884-1890, 2016. Available: 10.21275/v5i7.art2016624.
3) "MULTI-CLOUD MOBILE COMPUTING FOR SECURE STORAGE OF DATA USING CRYPTOGRAPHY", International Journal of Recent Trends in Engineering and Research, vol. 4, no. 4, pp. 608-611, 2018. Available: 10.23883/ijrter.2018.4280.uspsq.
4) S. Mohammad Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", Signal Processing, vol. 92, no. 5, pp. 1202-1215,

2012. Available: 10.1016/j.sigpro.2011.11.004.
5) V. Adat and B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", Telecommunication Systems, vol. 67, no. 3, pp. 423-441, 2017. Available: 10.1007/s11235-017-0345-9 [Accessed 8 October 2021].
6) M. Saleh and H. Hashim, "HYBRID CRYPTOGRAPHIC APPROACH FOR INTERNET OF THINGS APPLICATIONS: A REVIEW", Journal of Information and Communication Technology, vol. 19, no. 3, pp. 279-319, 2020. Available: 10.32890/jict2020.19.3.1.
7) L. Ma, X. Sun and W. Jin, "Symmetric–asymmetric hybrid encryption and decryption system based on chaotic iris phase mask and computer-generated holography", Optical Engineering, vol. 59, no. 08, 2020. Available: 10.1117/1.oe.59.8.083106.
8) V. Panwar, D. Kumar Sharma, K. Pradeep Kumar, A. Jain and C. Thakar, "Experimental investigations and optimization of surface roughness in turning of en 36 alloy steel using response surface methodology and genetic algorithm", Materials Today: Proceedings, 2021. Available: 10.1016/j.matpr.2021.03.642.
9) T. Patil and P. Kulhalli, "Symmetric Key Cryptography Algorithm for Data Security", International Journal of Trend in Scientific Research and Development, vol. -2, no. -2, pp. 586-589, 2018. Available: 10.31142/ijtsrd9444.
10) L. Knudsen, "Block Ciphers: Analysis, Design and Applications", DAIMI Report Series, vol. 23, no. 485, 1994. Available: 10.7146/dpb.v23i485.6978.
11) A. Jain and A. Pandey, "Multiple Quality Optimizations in Electrical Discharge Drilling of Mild Steel Sheet", Materials Today: Proceedings, vol. 4, no. 8, pp. 7252-7261, 2017. Available: 10.1016/j.matpr.2017.07.054.
12) "Cryptography: Theory and practice", Computers & Mathematics with Applications, vol. 30, no. 9, p. 125, 1995. Available: 10.1016/0898-1221(95)90225-2.
13) A. Jain and A. Kumar Pandey, "Modeling And Optimizing of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet", Materials Today: Proceedings, vol. 18, pp. 182-191, 2019. Available: 10.1016/j.matpr.2019.06.292.
14) B. Schneier, "Cryptography: the importance of not being different", Computer, vol. 32, no. 3, pp. 108-109, 112, 1999. Available: 10.1109/2.751335.
15) Jain, A. Yadav and Y. Shrivastava, "Modelling and optimization of different quality characteristics in electric discharge drilling of titanium alloy sheet", Materials Today: Proceedings, vol. 21, pp. 1680-1684, 2020. Available: 10.1016/j.matpr.2019.12.010.
16) S. Aboud, "Efficient Scheme for Obtaining Public Key Cryptosystem Using Shared Secrets", Information Technology Journal, vol. 6, no. 2, pp. 259-262, 2007. Available: 10.3923/itj.2007.259.262.
17) S. Bellovin and M. Merritt, "An attack on the Interlock Protocol when used for authentication", IEEE Transactions on Information Theory, vol. 40, no. 1, pp. 273-275, 1994. Available: 10.1109/18.272497.
18) S. Bahtiyar, "A Hybrid Trust-Modeling Approach for IoT Security", Electrica, vol. 20, no. 1, pp. 86-96, 2020. Available: 10.5152/electrica.2020.19090.
19) H. Sedjelmaci and M. Feham, "Novel Hybrid Intrusion Detection System For Clustered Wireless Sensor Network", International Journal of Network Security & Its Applications, vol. 3, no. 4, pp. 1-14, 2011. Available: 10.5121/ijnsa.2011.3401.
20) R. Kavitha and B. Caroline, "Hybrid Energy-Efficient Transmission Protocol for Heterogeneous Wireless Sensor Networks", Circuits and Systems, vol. 07, no. 06, pp. 897-906, 2016. Available: 10.4236/cs.2016.76077.
21) A. Yin and H. Liang, "Certificateless Hybrid Signcryption Scheme for Secure Communication of Wireless Sensor Networks", Wireless Personal Communications, vol. 80, no. 3, pp. 1049-1062, 2014. Available: 10.1007/s11277-014-2070.
22) K. Heung, A. Lashkari and A. Ghorbani, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced Artificial Intelligence", IEEE Access, vol. 5, pp. 3302-3312, 2017. Available: 10.1109/access.2017.2677520.
23) J. Mirza and M. Sharma, "A Hybrid Cryptographic Technique for Secured Authentication in Cloud Computing", International Journal of Computer Applications, vol. 141, no. 13, pp. 51-56, 2016. Available: 10.5120/ijca2016909797
24) Nagendra Kumar Maurya, Vikas Rastogi, and Pushpendra Singh, "Experimental and Computational Investigation on Mechanical Properties of Reinforced Additive Manufactured Component", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 6(3), 207-214 (2019). https://doi.org/10.5109/2349296
25) Ang Li, Azhar Bin Ismail, Kyaw Thu, Muhammad Wakil Shahzad, Kim Choon Ng, and Bidyut Baran Saha, "Formulation of Water Equilibrium Uptakes on Silica Gel and Ferroaluminophosphate Zeolite for Adsorption Cooling and Desalination Applications", Evergreen, 1(2), 37-45 (2014). https://doi.org/10.5109/1495162
26) Endah R Dyartanti, I Nyoman Widiasa, Agus Purwanto, and Heru Susanto, "Nanocomposite Polymer Electrolytes in Pvdf/Zno Membranes Modified with Pvp for Lifepo_4 Batteries", Evergreen, 5(2), 19-25 (2018). https://doi.org/10.5109/1936213
27) Hiroshi Naragino, Mohamed Egiza, Aki Tominaga, Koki Murasawa, Hidenobu Gonda, Masatoshi Sakurai, and Tsuyoshi Yoshitake, "Fabrication of Ultrananocrystalline Diamond/Nonhydrogenated Amorphous Carbon Composite Films for Hard

Coating by Coaxial Arc Plasma Deposition", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 3(1), 1-5 (2016). https://doi.org/10.5109/1657379

28) Mohamed Egiza, Hiroshi Naragino, Aki Tominaga, Kouki Murasawa, Hidenobu Gonda, Masatoshi Sakurai, and Tsuyoshi Yoshitake, "Si and Cr Doping Effects on Growth and Mechanical Properties of Ultrananocrystalline Diamond/Amor-Phous Carbon Composite Films Deposited on Cemented Carbide Substrates by Coaxial Arc Plasma Deposition", Evergreen: joint journal of Novel Carbon Resource Sciences & Green Asia Strategy, 3(1), 32-36 (2016). https://doi.org/10.5109/1657738
29) Ashish Kumar Srivastava, Shashi Prakash Dwivedi, Nagendra Kumar Maurya, and Manish Maurya, "3d Visualization and Topographical Analysis in Turning of Hybrid Mmc by Cnc Lathe Sprint 16tc Made of Batliboi", Evergreen, 7(2), 202-208 (2020). https://doi.org/10.5109/4055217
30) Dharu Feby Smaradhana, Dody Ariawan, and Rafli Alnursyah, "A Progress on Nanocellulose as Binders for Loose Natural Fibres", Evergreen, 7(3), 436-443 (2020). https://doi.org/10.5109/4068624
31) Matheus Randy Prabowo, Almira Praza Rachmadian, Nur Fatiha Ghazalli, and Hendrik O Lintang, "Chemosensor of Gold (I) 4-(3, 5-Dimethoxybenzyl)-3, 5-Dimethyl Pyrazolate Complex for Quantification of Ethanol in Aqueous Solution", Evergreen, 7(3), 404-408 (2020). https://doi.org/10.5109/4068620
32) Jain, Ankit, Cheruku Sandesh Kumar, and Yogesh Shrivastava. "Fabrication and Machining of Metal Matrix Composite Using Electric Discharge Machining: A Short Review." Evergreen, 8(4), 740-749 (2021). https://doi.org/10.5109/4742117