International Journal of Scientific Research in Multidisciplinary Studies
Vol.**10**, Issue.**4**, pp.**77-83**, April **2024**
E-ISSN: 2454-9312 P-ISSN: 2454-6143
Available online at: www.isroset.org

Review Article

A Recent Study on Security Techniques of Information Communication Systems

Joydeep Dey[1*], Sunil Karforma[2]

[1]Dept. of Computer Science, M.U.C. Women's College, Burdwan, India
[2]Dept. of Computer Science, The University of Burdwan, India

**Corresponding Author: joydeepmcabu@gmail.com*

Received: 10/Feb/2024; **Accepted**: 15/Mar/2024; **Published**: 30/Apr/2024

Abstract— Data security is a vital and challenging issue in this digitally revolutionary generation. Due to the attackers presence inside the open networks it is mandatory to protect any data before its transmission. Any online message communication must be ensured through cryptographic applications. Cryptographic applications are used to convert the plain text into cipher text by the sender and vice – versa by the receiver. In this paper, a recent study on the secure information communication had been conducted. The authors had reviewed twenty one research papers on the relevant cryptographic topics. Such papers were categorically divided into three sections. They are: cryptographic features, soft computing, and hybrid mode of encryption. It was observed that genetic algorithm, artificial neural network, fuzzy inference, etc were applied to ensure the data encryption technique. Soft computing is one of the major effective tools to generate secret key. The computing time calculation was tried to reduce by different authors through such techniques. Various mathematical tests were conducted by several authors.

Keywords— Cryptography, Data Security, Online Systems, Encryption, Decryption, Secret Key

1. Introduction

Secure message communication is needed in each and every online system. The sender must send the data in a much protected manner so that the intruders are not being able to decode it. There are so many applications areas such as cloud computing, IoT, IoV, WSN, networking, etc. Likewise, the telemedicine system is very must essential to ensure the confidentiality of the patients. Patients' medical data security is a very sensitive and critical issue for all types of telemedicine systems. Patients' secret data should be kept confidential and secure against the intruders. Thus, both the patients and the doctors should be given safety measure against such data attacks. Internet based technologies must be adopted by the healthcare providers in order to ensure their patient's data is always protected. Telemedicine is another method to provide health related treatments and services with the help of Internet technology. The patients can consult virtually with the physicians and can get their expert advice. It curtails the physical travelling costs. The significance of information security in telemedicine couldn't possibly be more significant. Patient's medical information must be kept private consistently in order to safeguard both the patients and the doctors. On the off chance that patient data is made to be compromised intentionally, it could lead to a lack of confidence and trust among the patients, as well as legitimate activity from the individuals who have had drained the information out. Patient's information is very much likewise important to programmers and other cyber criminals, who may involve it for monetary benefits or frauds. Along these lines, medical services suppliers should be cautious about safeguarding their patient data from unapproved access by carrying out powerful safety efforts across their frameworks as a whole and organizations.

Telemedicine has many advantages. They are stated as follows. Continuous remote monitoring of the patients can be done. Advanced IoTs are available to monitor such patients' data [1]. ECG, blood pressure, body temperature, etc are possible to monitor easily. IoT enabled cloud computing can be very much effective in the design of authentication protocols of the telemedicine. [2]

Clinical consultation in online mode can be done using telemedicine. Plenty of data communication can be shared for the research and education purposes through these telemedicine systems. The relevance of the patient's data security in online healthcare systems cannot be ignored at all. Patients' data must be placed away from the access of the intruders in order to protect both the patient's and the doctor's credentials. As the patients' data has plethora of its own importance, so it is always desirable for the hackers and other intruders, who use them for the financial profits. Therefore, the service providers of any online healthcare system should be attentive about protecting the patient's private information

against the intruders. This can be done by implementing strong data security measures across the public networks.

A secure online healthcare system should provide all such facilities likes of data confidentiality, data integrity, data authenticity, and data availability on the medical grounds. To ensure data privacy on these medical data, the term cryptography is the best suited option. Cryptography can make sure the confidentiality and integrity of different medical data while in transmission. It can also authenticate users against the intruders. Cryptography deploys encryption tools to protect the patients' confidential information. The selection of a strong secret key is the vital thing here. The converted cipher text will be used for transmission in the networks. It allows the remote users of the online system with high security to share their reports, data, etc to the others. Cryptographic application process may be of two types.

Symmetric key cryptographic algorithm i.e. the same secret key value shall be used in both the encryption and decryption phase [3]. DES, AES, RC5, RC6, 3DES, etc are its examples. Asymmetric cryptographic algorithm i.e. a different key pair is used during the encryption and decryption process [3]. RSA is a good example here.

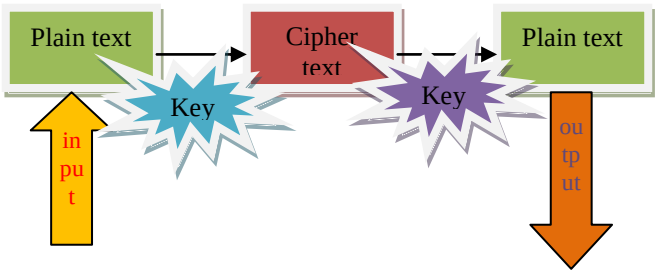

Figure 1.Basic model of cryptography

In the above mentioned figure 1, it is shown that plain text will be converted into cipher text using a key, and again the cipher text is being converted into the plain text using a key. The key is same in both the cases in case of symmetric key cryptography and different key pair is used in case of asymmetric key cryptography.

The following table 1 compares between three basic cryptography methods.

Table 1. Comparison between methods

Attributes	DES	AES	RSA
Year of Invention	1977	2001	1978
Cipher Text	Symmetric Block	Symmetric Block	Asymmetric Block
Size (Key)	56 bits	128 to 256 bits	1024 bits
Size (Block)	64 bits	128 bits	Not fixed
Rounds	16	10-14	1
Speed of the method	Slow	Fast	Slow
Power consumption	Low	Low	High

From the above noted table 1, it can be stated that RSA asymmetric key algorithm needs higher power consumptions against DES and AES. But AES symmetric key algorithm is a fast method between these two. Depending on the needs of security, the exact algorithm is being selected for the online communication systems.

One more important issue is the session key management here. On the onset of COVID-19, the volume of online transactions had excessively triggered in the last couple of years. More we generate a strong session key, more secure is our technique. Intruders are always in active mode to leak that session key. Once it gets leaked out, the entire transactions will e available to the external intruders. This part of session key generation has to be handled with care and priority. Many researchers are continuously working in this domain to protect different types of confidential data and transactions. Despite of that intruders have made a strong emphasis on the online data hacking and its threats. There are so many types of data security threats on the online application systems. Data security is a major concern for its all users. In the online healthcare systems the data is either stored on or carried forwarded to the next communication networks. The data intrusion is the biggest challenge that needs to be addressed soon. With the emerging internet based cryptographic tools and algorithms it can e achieved with better efficacy. Following are the major threats over here.

a) DATA BREACHES

Breaching on the medical data is done when the external agents and intruders get unapproved information access facility on different types of stored data. Data breaching is the outcome of malware attacks, social engineering, phishing attacks, and ransomware attacks, etc. Intruders are financially gained by selling such crucial data. The chances of such data breaching gets higher with the rise in the implementation of online healthcare systems.

b) INSIDER THREATS

The employees of an organization are also another type of vital threat to the data security system. They always have legitimate access to the patient's files and other sensitive data of the healthcare system. Software glitches, human errors, negligence, rogue employees may lead to data breaches which can supply the credentials to the intruders.

c) DENIAL OF SERVICE ATTACKS

Fake network traffics are being put into the organization's computer traffic physically by overloading them. Thus, hackers can gain the vital users data. Thus, data can be made stolen that is not at all desirable.

d) PHISHING SCAMS

Phishing means to redirect the users to some risky websites and will ask them to share their credentials. The best technique to avoid phishing scams that users should know how each healthcare service provider will contact the users and patients and rejecting all suspicious requests for sensitive information.

e) ADVANCED PERSISTENT THREATS (APT)

Social engineering scams are mainly caused through advanced persistent threats. It is nothing but to steal the private and sensitive information by the help of malware silently kept on the public computer networks. Such kind of organized crimes are conducted by the skilled hackers for different wrong intentions.

f) ROGUE EMPLOYEES

The employees of any organization who intentionally used to violate or sell their organization's secure information and other confidential policy mechanisms are a dangerous threat of concerns. The concerned organization shall go it

g) MOBILE THREATS

Mobile devices allow private access to the patients' health information and online education easier. It also introduce newer and challenging problem of data security. Mobiles and other portable devices are being easily compromized by the intruders and hackers to fetch the private data. Preventative measures sometimes failed that include encryption, roust secret key, secure Internet browsing, password protections (OTP), etc for protecting mobile devices.

h) UNSECURE USER DEVICES

High popularity of different online apps could expose more personal data to the hacking attackers due to less system protection. Firewall is one popular ay to prevent the unwanted access. Users should always log in through secure systems rather public systems.

i) INTERNET OF THINGS (IOT) THREATS

The increase in the number of Internet dependent devices has developed a newer level of different security challenges likes of ransomware attacks on computers, desktops, laptops, smart TVs, mobiles, etc. Internet of Things (IoT) are low processing sensors and it needs a different style from traditional data security preventive measures. IoT devices are very sensitive and can easily be trapped by the intruders. The more connected our digital world becomes then it is very easier for the intruders to access valuable credentials like personal records and data.

Section 1 contains the introduction of the entire review paper with different security aspects. Section 2 consists of literature review. Section 3 defines the summary and conclusions.

2. Review of Literature

In this section, the authors had reviewed twenty one (21) research papers on the relevant topic which includes research publications from IEEE, Springer, Elsevier, etc. The authors had categorically divided into three groups. First group consists of research papers related to the cryptographic features on the telemedicine systems. Second group contains the research papers based on soft computing. Soft computing includes Artificial Neural Network (ANN), Genetic Algorithms, Fuzzy logic, Machine Learning, Deep Learning, etc. Last group includes the papers on hybrid computation. In the following paragraphs, detailed analysis of such research papers shall be presented.

Chen C.K. et al. [4] had presented an experimental study on improved chaotic synchronization for the secure data communication purpose. They had used Lorenz equations in the key generation process. Biometric authentication is strong tool in telemedicine. ECG signals are very much unique to generate secret keys. They had designed two electrode based hand held ECG detectors. Lorentz based chaotic circuit will acquire the ECG signals and generate the key. Encryption and decryption can be done with the same key. They have tested their manuscripts to generate the cipher text file also. Different image dimensions were used in their chaotic encryption phase. Shaikh M. et al. [5] had designed the ECG signal encryption and decryption process on homomorphic encryption. Since the patients' heartbeat is an essential parameter so they had considered QRS complex of the ECG signal. This portion will detect whether the patient is suffering from any cardiac issues or not. They had used the ECG database from MIT-BIH Arrhythmia database at 360Hz sampling frequency. A group of encryption functions with algebraic functions were used here. They have calculated threshold encryption values at two signal points as C1 and C2 and E is their homomorphic encryption. 52.17 was the heart rate as decrypted by their system which is not normal value. Popescu A.B. et al. [6] had proposed a homomorphic encryption model on real numbers to protect the patients' data. They had evaluated their scheme on two real world EEG data for seizure detections and prediction of predisposition to alcohol addiction. Supervised based machine learning and direct fitting methods were used manage their computations. The EEG dataset which was used by them had five hundred files. Each of them connected with 23.6 sec of EEG at 173.61 Hz sampling rate [7]. Their machine learning algorithm had five outputs as follows: epileptic seizure activities, tumor zone, healthy human brain area with an identified tumor, patients having their eyes closed during the EEG recording, and patients had their eyes open during the EEG recording. Son S. et al. [8] had designed an authentication mechanism on cloud computing based TMIS. Smart wearable have very less memory capacity which has been addressed here by them. They have deployed cipher text-policy attribute-based encryption (CP-ABE) to create access control mechanism for the medical data storage inside such cloud servers, and block chain was being used to guarantee data integrity. They had validated their proposed method by using an automated validation of internet security protocols and applications (AVISPA). Zhang A. et al. [9] had proposed block chain secure patients' data sharing scheme. Two types of block chains were constructed here. Firstly, private block chain and consortium block chain were constructed according to their defined data structures and consensus mechanisms. The private block chain was to store the medical data and the consortium block chain was used to record the secure indices of the medical data. Security analysis had shown that their proposed protocol have met with the security targets. Yang X. et al. [10] had developed a secure medical information sharing based on the attribute cryptographic system and the block chain technique. Their cipher texts were stored inside the clouds, and addresses of the storage were written in the block chain. Their results had shown that it had satisfied the confidentiality and non- tampering with better computational

performances. The patients' data were preserved in secure way through clouds. Nagasubramanian G. et al. [11] had developed a cloud system to have an authentication mechanism and data integrity to the medical data. Keyless digital signature was used in their method. The proposed block chain has been done to have data integrity. Their response time has been reduced to 50% with respect to other conventional methods. 20% cost reduced I their data storage system. Cubo E. et al. [12] had highlighted the recent outcomes of treating Pakinson's disease through telemedicine. They had surveyed the challenges and positive outcomes of such online treatment mode. Telemedicine is a promising tool to treat remote patients with neurological issues.

Madhiarasan M. et al. [13] had proposed a multilayer-perceptron based neural-network which works on the solar irradiance forecasting model, an enriched back-propagation artificial neural network oriented rainfall forecasting model and an Elman artificial neural network based on the temperature forecasting model. Their outcomes of the proposed models were analyzed in details with several hidden neurons and then validated by using the obtained real-time meteorological information. They have developed their models with 05 years, 05 years, and 07 years data sets for the solar irradiance, rainfall prediction, and temperature forecasting applications, respectively. The inter-annual variability-based uncertainty can be minimized by their technique. The proposed forecasting models have minimum design issues with minor error qualifiers. Vanegas-Ayala S.C. et al. [14] had developed a predictive model with the help of fuzzy inference systems. They had predicted indoor relative humidity values inside the greenhouse having greater accuracy and interpretability rates. They have found that in the proposed six models that clearly defined the behaviours of the humidity as an outcome of temperature, carbon dioxide, and soil moisture with percentage of effectiveness greater than 90%. They have used Mamdani-type fuzzy inference system along with an optimized hybrid technique of genetic and interior point algorithms. It had helped them to predict the relative indoor humidity values in the greenhouses with higher interpretability and higher precision. They had observed an effective percentage of 90.97% and Mean Square Error (MSE) of $8.2e-3$. Raymond J.L. et al. [15] had specified that the recent inventions indicate the cerebellum implements supervised learning by using the following organizational rules: extensive pre-processing of the inputs representation i.e. feature engineering, recurrent circuit architecture, linear I/O computations, sophisticated instructive signals which may be regulated and are predictive, adaptive mechanisms of plasticity with multiple timescales, and problem-specific hardware specializations. The principles emerging from the studies of the cerebellum have striking parallels with those in other brain areas and in the artificial neural networks, as well as a good number of notable differences that can inform the direction of the future research on supervised learning and inspire the next-generation machine- based algorithms. Chai H. et al. [16] had proposed a logistics regression model on complementary of active learning and semi-supervised learning. They had utilized the unlabeled data samples having minimum costs to enhance the disease classification accuracy. An improved pseudo-labelled samples mechanism has been developed to curtail the false pseudo-labelled samples. The experimental results had shown that it may achieve better performances as compared to the widely used semi-supervised learning and active learning methods for the disease segregation and gene selection problems. Das A. K. et al. [17] had proposed direction-based exponential mutation operator for coding genetic algorithm (GA). Their new developed mutation operator has been influenced by the directional data of the design variables here. They had tested their operator on 20 classical benchmark optimization problems. They had also compared their outcomes with polynomial mutation operator. In majority of the cases they had achieved better results. It was an efficient technique in that domain. Hussain A. et al. [18] had proposed a newer crossover operator for the traveling salesman problem to find out the minimum distance. Different crossover operators have been presented here with respect to travelling salesman problem. They had applied all three proposed crossover operators on different benchmark problems. It was found that the proposed operator had worked over 20, 70, and 100 percent for ft53, dantzig42, and ftv170 problems, respectively, when they were compared to the other two operators. Moreover, the researchers will be more confident to use it for comparisons also in future. Arshad M. et al. [19] had proposed a technique to update the encryption with customized the genetic algorithm (GA) with added flavors of data encryption. Their enhancements on the randomness of the proposed key generated were done by altering the population size, number of generations, and mutation rate. The first step of data encryption was to convert the sample data into the equivalent binary data. They had used local intelligence to generate the random bits. Their results had displayed that the proposed technique was at least 80% efficient in terms of computing time while generating the encryption key with the same randomness status as generated by some conventional GAs.

In this final paragraph, detailed review of studies has been done on the hybrid computation. Bane P. et al. [20] had presented a multilevel theory of cryptographic model using S-DES key generation process and genetic algorithm. Their proposed method has the dynamic key length and variable output size. It can provide 2256 number of alternative keys, which is very much difficult to break. They have shown that their method had exhibited better outcomes than the classical methods. Jawaid S. et al. [21] had used soft computing skills to generate the secret key. Genetic algorithm was implemented to have randomized secret key. Autocorrelation test was used to measure the randomness of their proposed secret key. They had implemented through Java language and had obtained satisfactory results. Thus, secure data communication can be achieved by their proposed design. Jawaid S. et al. [22] had generated nature based secret key using genetic algorithm. They have used DES encryption with their proposed key. The proposed keys were very much difficult to decode by the intruders. Such keys were very much complex and random in nature. Their approach had seven rounds and the entire process was repeated for hundred times. The secret key can be generated in a very short period

of time that proved as an advantage in the segment of computational time. de Campos Souza P.V. et al. [23] had used a hybrid model to recognize the anomalies in digital and Internet transactions. They had used artificial intelligence model which can show relationship between the fuzzy logic and the training data. They have achieved 99% accuracy in the anomaly detection inside the networks. Their proposed fuzzy based neural network has attainment of the best training and test accuracy percentage which allows the best ability to identify the digital attacks in this online era. However, it was recorded that their training and testing accuracy time was much greater when compared with the other models of the cyber invasion. Despite of having more training time needed here, the proposed method had shown the best results against the other methods. Jain G. [24] had proposed genetic algorithm based key generation which can better be used against the classical encryption methods. They had implemented data security tightness on the cloud computing domain. Users' credentials must be preserved in this Internet friendly era. They had given emphasis on the standard parameters of their encryption method in terms of execution time, throughputs, and secret key size. They had tested these parameters for correlation of their proposed method. It had also compared the proposed methodology with the existing cryptographic algorithms likes of AES, RC5, RC6, Blowfish, DES, 3DES, etc.

3. Material and Method

Twenty one (21) research papers were reviewed from international research publications such as IEEE, Springer, Elsevier, etc. The data security system was the integral theme while searching the papers. The inclusive criterion was to select the papers which were published within last ten years. Such selected papers were divided into three separate categories. First one is the research papers related to the cryptography and its knowledge on the telemedicine systems. Second one is the research papers based on soft computing that includes Artificial Neural Network (ANN), Genetic Algorithms (GAs), Data Mining, Fuzzy logic, Machine Learning, Deep Learning, etc. Last one includes the papers on hybrid computation.

4. Summarized Results

The authors have reviewed the above stated research papers with the following classifications. The total number of review papers was twenty one.

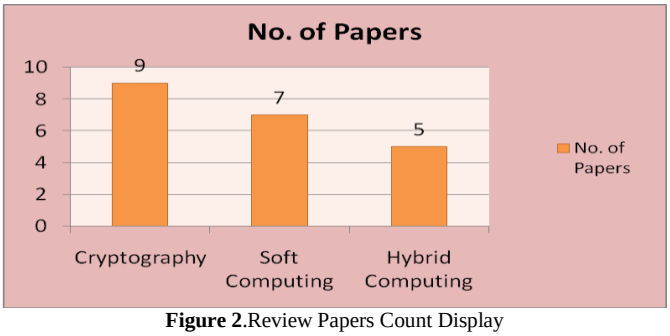

Figure 2.Review Papers Count Display

From the above noted figure 2, it is found that the authors had reviewed nine papers on the cryptography, seven papers on the topic of soft computing, and five papers on the hybrid mode of computing.

The authors had made an extensive search with different keywords on the Internet sources from the publications within last ten years. They had listed some of the important keywords in the following table 2.

Table 2. Used Keywords

Publication Year	Internet Sources	Search Keywords
2013-2023	Science direct, Scopus, Google scholar, ACM, IEEE xplore, ISROSET, IJSRMS	Cryptography, Data security, E-health privacy, Session Key Management

Different searching keywords were followed by the authors to find out the relevant research papers. They had used different searching word combinations on the Internet sources. Sometimes they had been successful and sometimes not. In case of failures, they had to retry with different combination of keywords on the relevant topic of study.

5. Conclusions and Future Scope of work

In this section, the author had tried to summarize his observations. In this paper the author had reviewed twenty one research papers. Cryptographic mechanisms were applied on the telemedicine system. The authors [4, 5] had used ECG signals their studies. ECG signal is very critical parameter and it needs to be secure. The author [5] had used Lorenz equations in their key generation procedure. The author [2] had used homomorphic encryption in their paper for encrypting and decrypting the ECG signals. EEG signals were also used by the other authors for the purpose of patients' security. Medical data can be recorded through block chain also by some authors [8, 9]. Cloud computing is also a mechanism to ensure patients' authentication.

Soft computing is very much important to deploy security features on the telemedicine system. In the manuscripts [10, 12] the authors had used artificial neural networks to predict the data. In [11], predictive model with the help of fuzzy inference systems was used. They have used Mamdani-type fuzzy inference system along with an optimized hybrid method of genetic and interior point algorithms for weather forecasting. The author [13] had utilized semi- supervised learning to classify the diseases with unlabeled data samples with minimum cost. The authors [14-16] had applied genetic algorithm to solve different optimization problems. They had obtained better results when compared with conventional algorithms. Thus, soft computing based encryption was applied in an efficient way.

Hybrid mode of encryption has been noted as a significant contribution by different authors also. In the papers [20, 21, 24], the authors had intelligently applied soft computing and genetic algorithm. The author [20] had generated dynamic key lengths. 2256 number of alternate keys was proposed.

Random secret key was designed with autocorrelation [21]. Cloud computing was used to enhance the data security features. AI and fuzzy were also applied by the authors [24]. Mortada M. et al. [25] had developed wireless monitoring system for the human body by the help of electronic face mask in the field of healthcare. Mortada M. et al. [26] had designed sensors for the system to manage the automatic car parking. It was a very useful method.

In future, the authors shall try to review more research papers purely based on machine learning and deep learning on different real time applications. ML based papers reveals higher accuracy in their proposed models.

Data Availability: Twenty one research papers are available. On reasonable requests, it can be made available to them if needed only.

Conflict of Interest: No conflict of interest is there between the authors in this paper.

Funding source: Authors do not receive any research grants.

Author's contribution: Both the authors had equally contributed and checked the entire paper.

Acknowledgment: Authors do acknowledge the efforts spent by the Editor(s) and Reviewer(s) in this paper.

References

[1] Joel J. P. C. Rodrigues, Dante Borges De Rezende Segundo, Heres Arantes Junqueira, Murilo Henrique Sabino, Rafael Maciel Prince , Jalal Al-Muhtadi , Victor Hugo C. De Albuquerque, "Enabling technologies for the internet of health things", IEEE Access, Vol 6:13129–13141, 2016.

[2] Geeta Sharma, Sheetal Kalra, ''A lightweight user authentication scheme for cloud-IoT based healthcare services,'' Iranian J. Sci. Technol., Trans. Electr. Eng., vol. 43, no. S1, pp. 619–636, Jul. 2019.

[3] Bruce Schneier, "Applied Cryptography", John Wiley & Sons Inc., New York, USA, 2nd edition, 1996.

[4] Ching-Kun Chen, Chung-Liang Lin, Shan Lung Lin, "Data Encryption and Transmission Based on Personal ECG Signals", International Journal of Sensor Networks and Data Communications, Vol 4, Issue-2: pp:1-13, 2015.

[5] Muhammad Umair Shaikh, Siti Anom Ahmad, Wan Azizun Wan Adnan, "Investigation of Data Encryption Algorithm for Secured Transmission of Electrocardiograph (ECG) Signal", IEEE-EMBS Conference on Biomedical Engineering and Sciences (IECBES), Sarawak, Malaysia, pp: 274-278, 2018.

[6] Andreea Bianca Popescu et al., " Privacy Preserving Classification of EEG Data Using Machine Learning and Homomorphic Encryption" , Applied Science, Vol: 11, Issue:16, pp: 7360, 2021.

[7] Dheeru Dua, Claus Graff, "UCI Machine Learning Repository", 2017, Available online: http://archive.ics.uci.edu/ml (accessed on 21 December 2023).

[8] Seunghwan Son , Joonyoung Lee, Myeonghyun Kim, Sungjin Yu, Ashok Kumar Das, Youngho Park, "Design of secure authentication protocol for cloud- assisted telecare medical information system using blockchain", *IEEE Access* ,Vol *8*, pp: 192177–192191, 2020.

[9] Aiqing Zhang , Xiaodong Lin., "Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain", Journal of Medical Systems, vol 42, pp:140, 2018.

[10] Xiaodong Yang, Ting Li , Xizhen Pei, Long Wen, Caifen Wang, ''Medical data sharing scheme based on attribute cryptosystem and blockchain technology,'' IEEE Access, vol. 8, pp. 45468–45476, 2020.

[11] Gayathri Nagasubramanian, Rakesh Kumar Sakthivel, Rizwan Patan, Amir H. Gandomi, Muthuramalingam Sankayya, Balamurugan Balusamy, "Securing e-health records using keyless signature infrastructure blockchain technology in the cloud", Neural Computing & Applications, Vol 32, pp:639–647, 2020.

[12] Esther Cubo , Pedro David Delgado-López, "Telemedicine in the Management of Parkinson's Disease: Achievements, Challenges, and Future Perspectives", *Brain Science, Vol 12, pp:* 1735, 2022.

[13] Manogaran Madhiarasan' Mohamed Louzazni, "Analysis of Artificial Neural Network: Architecture, Types, and Forecasting Applications", Journal of Electrical and Computer Engineering, vol. 2022, pp: 23, 2022.

[14] Sebastian-Camilo Vanegas-Ayala, Julio Barón-Velandia, Daniel-David Leal-Lara, "Predictive Model of Humidity in Greenhouses through Fuzzy Inference Systems Applying Optimization Methods", Advances inFuzzy Systems, vol. 2023, pp: 22, 2023.

[15]Jennifer L Raymond , Javier F Medina, "Computational Principles of Supervised Learning in the Cerebellum", *Annual Review of Neuroscience, Vol 41*, pp: 233– 253, 2018.

[16]Hua Chai, Yong Liang, Sai Wang, Hai-wei Shen., "A Novel Logistic Regression Model Combining Semi- Supervised Learning and Active Learning for Disease Classification:, *Scientific Reports*, Vol *8*, pp: 13009, 2018.

[17] Amit Kumar Das, Dilip Kumar Pratihar, "A Direction-Based Exponential Mutation Operator for Real-Coded Genetic Algorithm," *2018* Fifth International Conference on Emerging Applications of Information Tech*nology (EAIT)*, Kolkata, India, pp: 1-4, 2018.

[18] Abid Hussain, Yousaf Shad Muhammad, M. Nauman Sajid, Ijaz Hussain, Alaa Mohamd Shoukry, Showkat Gani , "Genetic algorithm for traveling salesman problem with modified cycle crossover operator", Computational Intelligence and Neuroscience, Vol 2017, pp:1–7, 2017.

[19] Muhammad Junaid Arshad, Muhammad Umair, Saima Munawar, Nasir Naveed, Humaira Naeem, "Improving Cloud Data Encryption Using Customized Genetic Algorithm". International Journal of Intelligent Systems and Applications, Vol 12, pp:46-63, 2020.

[20] Pooja Bagane, Deepak Dharrao, S. Kotrappa, "Multilevel Approach for Cryptography using Genetic Algorithms with Existing S-DES Key Generation Method", *Int J* Intelligent Systems and Applications in Engineering, vol. 10, issue. 4, pp: 701–706, 2022.

[21] Sania Jawaid, Anam Saiyeda, Naba Suroor, "Selection of Fittest Key Using Genetic Algorithm and Autocorrelation in Cryptography", Journal of Computer Sciences and Applications, Vol 3, issue 2, pp: 46-51, 2015.

[22] Sania Jawaid, Jamal Adeeba, "Generating the Best Fit Key in Cryptography using Genetic Algorithm", International Journal of Computer Applications, Vol 98, pp: 33-39, 2014.

[23] Paulo Vitor Campos Souza, Fonda, Augusto Junio Guimarães, Thiago Silva Rezende, Vinicius Jonathan Silva Araujo, Vanessa Souza Araujo, "Detection of Anomalies in Large-Scale Cyberattacks Using Fuzzy Neural Networks" *AI, Vol* 1, issue 1, pp: 92-116, 2020.

[24] Garima Jain, "Genetic Algorithms with Cloud Computing for Data Security & Performance Enhancements", Journal of Education: Rabindrabharati University, Vol XXIII,issue 11, pp:21-29, 2021.

[25] Mortada M. Abdulwahab, Khalid H. Ahmed, Hamza M. Al-mehrabi, Mohammed A. Al-kateb, Yazid A. Al-mezgagi, Jwher Y. Al-rashdi, "Design of Wireless Monitoring System of Body Health Using Electronic Face Mask," *World Academics Journal of Engineering Sciences*, Vol. 9, issue.2, pp.46-51, 2022.

[26] Mortada M. Abdulwahab1, Abdalrhman A. Mohammed, Abdalrhman H. Mohammed, Mohammed M. Hamza, "Design of Wireless Sensor System of Monitoring and Controlling Parking Cars," *World Academics Journal of Engineering Sciences*, Vol.9, issue.1, pp.18-22, 2022.

AUTHORS PROFILE

Joydeep Dey pursed Bachelor of Computer Application (Honours) from Cyber Research & Training Institute, Burdwan, India in 2007 and M.C.A. from the University of Burdwan in 2011 and he had secured First Class First (GOLD MEDALIST). He is working as State Aided College Teacher & Head in Department of Computer Science at M.U.C. Women's College, Burdwan since 2011. He has published 06 SCI indexed Springer journal papers , 08 SCOPUS Indexed journals, 04 Edited Book Chapters, (SPRINGER / ELSEVIER; SCOPUS INDEXED),06 International Conferences journals, and 35 others publications (International / National / State / Regional Level). His main research interest includes Cyber Security and Computational Intelligence in Telehealth domain. He has than 13.5 and 0.5 years of teaching experience at UG and PG level respectively.

Sunil Karforma has completed his Bachelors in Computer Science & Engineering, and his Masters in Computer Science & Engineering, from Jadavpur University. He received his Ph.D. in Computer Science, and is presently Professor of the Dept. of Computer Science at the University of Burdwan, India. His research interests include Network Security, E-Commerce, and Telemedicine. He has published 250 papers in both national as well as international reputed journals and conferences.

