Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 9
September 2023

Concepts Of Decoding in Cryptography

Naman Thakur,
Dept. of Computer Science & Engineering Chandigarh University, Gharaun-140123

Steve Samson,
Dept. of Computer Science & Engineering Chandigarh University, Gharaun-140123

Reeta Rautela
Uttaranchal University, Dehradun Email: reetarautela@uumail.in

Kavita,
Uttaranchal University, Dehradun Email: kavita@ieee.org

Abstract—The internet has arrived at such a stage that it has merged with our daily life, enlarging rapidly in the last few years. Data security and privacy has become a main risk and threat to everyone who is using or surfing over the internet. Data privacy and security makes sure that data should only be accessible by the authorized user & prevents the alteration and modification of message or data. So as to attain this level of protection and security, various methods and algorithms are developed. Cryptography is a technique of securing data with the help of algorithms, so that only the intended user can process and access that data. The letter suffix 'graphy' stands for 'writing' and 'crypt-' means 'hidden'. Cryptography is defined as the method that cipher information, depending on particular algorithms and codes make the info unreadable to the human eyes unless it is decrypted back by the codes that were pre decided by the client/sender . Cryptography is the technique of writing secure messages and data. Cryptographic algorithms are used to maintain the accounting and integrity of a system. The fundamental usage of cryptography is the capability to transfer data and messages between two parties in such a way that data is inaccessible to the unintended users. This project will be able to convert web application based encryption and decryption which convert confidential data into unreadable form by using various encryption techniques i.e converting plain text into hashing format). Base32, Base64, Base84 etc. are the few examples of base encryption techniques.

Index Terms—Cryptography, Encryption, Decoding, Security, Decryption

I.

INTRODUCTION

Data privacy and security has become the foremost facet while transportation of data and information [1]. The exchange and transmission of information, images, videos and docu- ments all needed data security and privacy from unauthorized users [2], [3]. Cryptography is the technique of writing secure messages and data [4], [5]. Cryptographic algorithms are used to maintain the accounting and integrity of a system. The fundamental usage of cryptography is the capability to transfer data and messages between two parties in such a way that data is inaccessible to the unintended users. Fig.1 tells the data is transferring between sender or client and receiver or server. Fig.3 indicates the interrupt is sitting b/w sender and receiver and interrupt is stealing and deleting the information between the two parties [6], [23]. Figure 2 below shows the communication between sender and receiver.

Cryptography is the algorithm of mathematics to encrypt and decrypt the data [7], [24]. The technology we are using in this project is encoding. Encoding is the technique of converting the data from one format to another format. There is a difference in Encryption , Encoding and Hashing [8], [25]. Encrypted data can be converted back to its normal form while a hashed value can't be converted back to normal form. So Encryption ensures confidentiality while hashing ensures integrity. A hash function

is used to generate a new value according to the algorithm [9], [26].

Cryptography plays an important role in achieving the main goals of cybersecurity, like confidentiality, integrity, non- repudiation and authentication. Cryptography algorithms and codes are designed to achieve this goal [10], [30]. Cryptog- raphy has the important role in maintaining and providing a powerful, robust network and reliable data privacy and security. The research has been successfully completed [11], [29]. The calculations in this research concludes that the Base algorithms are also good at information security systems for decryption and encryption as well [12], [28]. Figure 2 show how the interrupt sitting between sender and receiver can possibly do.

II. LITERATURE REVIEW

Susan al. indicates that computer & network security is rapidly increasing technology in the domain of computer science and digital information, with computer and network security learning cannot be stopped. Algorithmic codes and mathematical techniques, like encryption and hashing tech- niques, are the most focus of information and cyber security courses. As hackers are finding new ways and techniques to hack computers and networks, new certificates, courses and training are created that will cover the newest kind of web vulnerabilities and cyber attacks, but those vulnerabilities and attacks are also becoming outdated everyday due to the responses and patches from security teams [13]. Data privacy and security makes sure that data should only be accessible by

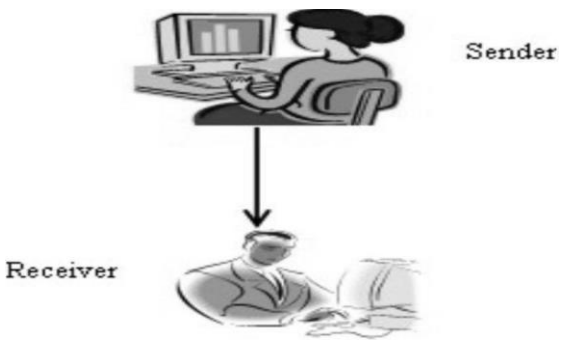

Fig. 1. Communication between Sender and Receiver

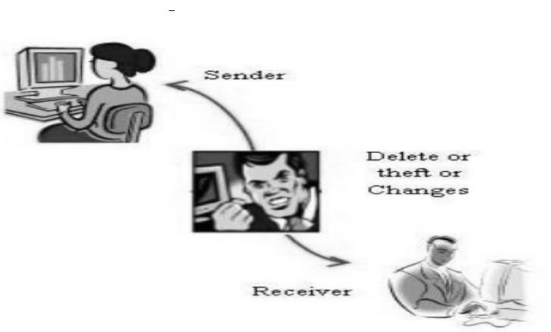

Fig. 2 The interrupt is sitting b/w sender and receiver the authorized user & prevents the alteration and modification of message or data. So as to attain this level of protection and security, various methods and algorithms are developed [14]. Khalifa Othman[v] indicated the first main concepts, goals & characteristics of cryptography. He wrote that in the present age, which is this present generation of information and digital data, communication and transmission has promoted the expansion of the technology & that's why it has a very vital role that needs data privacy of the user to be secured and making sure that when information is transferred through the means of communication [15], [31].

Jirwan Nitin [vi] demonstrated that information and data communication depends mostly on transfer of data over the internet, in which integrity and security has most importance while using the encryption and hashing algorithms in order that information and digital data should reach the receiver end securely without intervention and modification [16]. Nitin also referred to the other several algorithms and codes that have been used in the process of digital transmission, like asymmetric and symmetric method. Nitin also tells us that how people are using cryptographic algorithms will be deciding the future of data privacy, that basically depends on laws and regulations & traditions also, what is the current world expecting to attain [17].

In a research on cryptography and cyber security, Tayal Sandeep indicated that with the development of commerce applications and software, large amounts of digital data and information is being produced everyday by individuals and companies all over the globe. It made data privacy and security an enormous issue and threat in the matter of making sure

that the transmission of information through the internet is safely delivered. As more people are using the web, it further signifies the need for cryptographic algorithms and codes [18].

Gupta Anjula [viii] refers to the beginning & definition of cryptography and how data security and privacy is a difficult challenge in the age of the internet and computers. Addition- ally, cryptography is another way to make sure integrity, au- thentication, confidentiality & availability of the people and its digital data and information by ensuring privacy and security. This research also included other cryptographic algorithms and code that has provided the technique and methods to secure the users data. In addition, the future of cybersecurity and cryptography depends on a governing system producing strong and encrypted keys to confirm that only the intended and authorized user with the correct key should gain access to it, while other people without the correct keys can't access [19]. Callas J. refers to the topics like network security, pri- vacy strengthening technologies, cryptography, legal changes connecting the reliability, cryptographic technologies that are useful in dataprivacy improvement. Callas writes that how people are using cryptographic algorithms will be deciding the future of data privacy, that basically depends on laws and regulations & traditions also, what is the current world expecting to attain[29-35]. Callas noted that several gaps are in the domain of cryptography for future developers and researchers to fill [20]. In addition, the future of cybersecurity and cryptography depends on a governing system producing strong and encrypted keys to confirm that only the intended and authorized user with the correct key should gain access to it, while other people without the correct keys can't access. Finally, he demonstrated that people's thought and perspectives about communication privacy and security is a mirror of the changes that happen in cyber laws that come into acutality through incidents like the terrorist attacks of 9/11.

Anjula Nitin [x] tells us that As hackers are finding new ways and techniques to hack computers and networks, new certificates, courses and training are created that will cover the newest kind of web vulnerabilities and cyber attacks, but those vulnerabilities and attacks are also becoming outdated everyday due to the responses and patches from security teams. This research also included other cryptographic algorithms and code that has provided the technique and methods to secure the users data. It made data privacy and security an enormous issue and threat in the matter of making sure that the transmission of information through the internet is safely delivered. As more people are using the web, it further signifies the need for cryptographic algorithms and codes [21].

III. METHODOLOGY

The conversion of Base encoding is one of the algorithm for encode & decode the message into ASCII format, Base encod- ing and decoding is established on the number 32,82.64.91,. The words developed from Base include '0..9','A...Z' and 'a. . . z' '+' & '/' are the last two characters.

The Base64 encoding & decoding algorithm is easy and straightforward as shown in figure 4 and 5 below. There are some steps to achieve the Base algorithm: Check for the ASCII code of every letter as shown in figure 3 below. Search the binary number eight bits of existing ASCII code.

1) Add the last 8 bits to 24 bits

2) Divide the earlier 24 bits to 6 bits It'll generate 4 fractions

3) Every section is then transformed into a decimal value

4) In last convert these to characters with the help of index table

IV. RESULT

The data is a sensitive part of any people and organization. Any threat or loss to data can prove to be a great damage to the people and organization as well. These days sharing the data on the internet is becoming a huge concern due to privacy and security problems. Hence more algorithms and techniques are needed to secure the shared information in an unsecured channel like the internet. This research focuses mainly on a combination of different cryptography algorithms to protect the data and

information while sending over the internet. We all know how important defending and protecting personal data and information is to users and organizations, that's why all data and documents must be encrypted in a secure way so that only the intended user gets access to it.

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Fig. 3. Fig3. ASCII Table

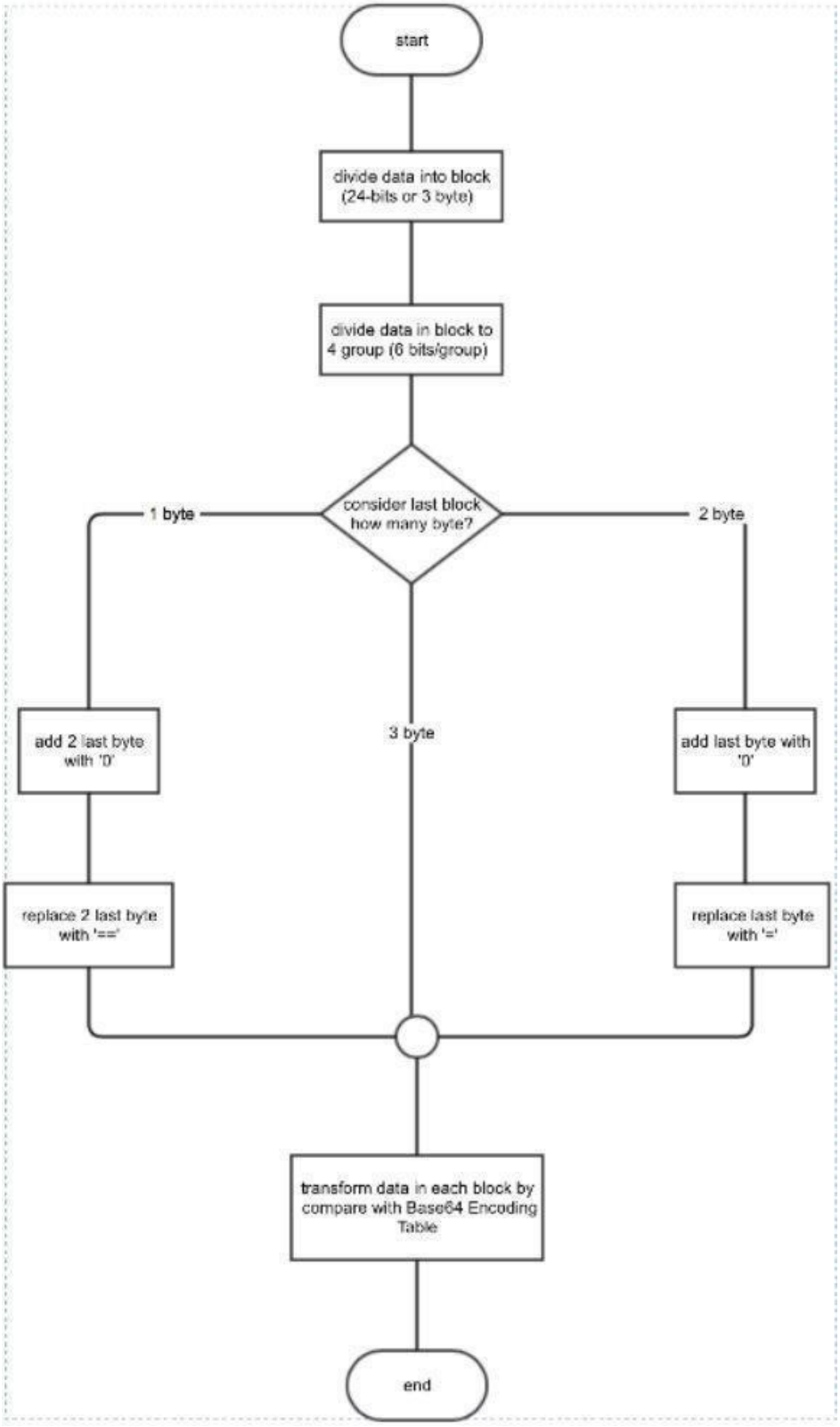

Fig. 4. Encoding Flowchart of Base64

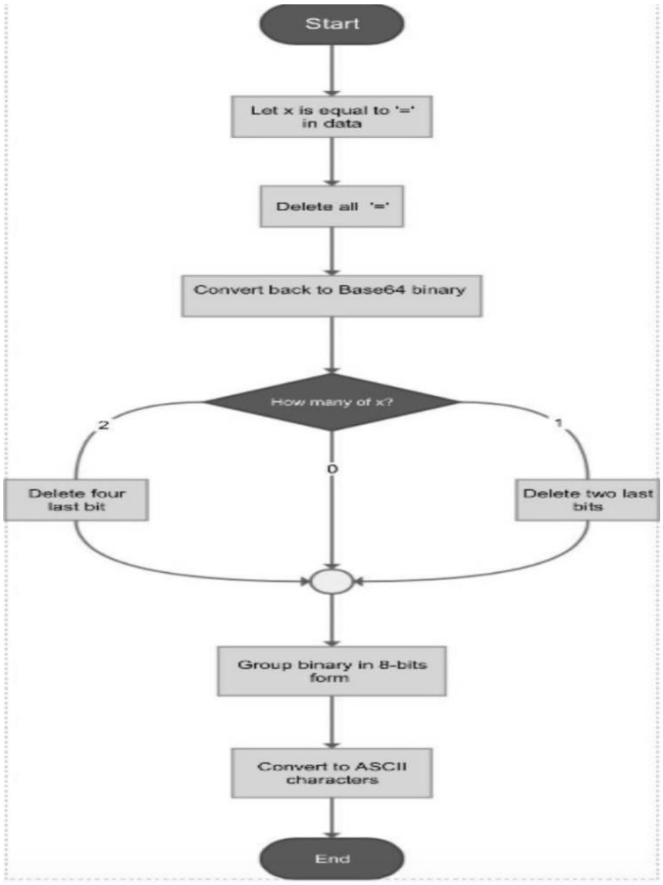

Fig. 5. Encoding Flowchart of Base64

V.

CONCLUSION

Cryptography plays an important role in achieving the main goals of cybersecurity, like confidentiality, integrity, non- repudiation and authentication. Cryptography algorithms and codes are designed to achieve this goal. Cryptography has the important role in maintaining and providing a powerful, robust network and reliable data privacy and security. The research has been successfully completed. The calculations in this research concludes that the Base algorithms are also good at information security systems for decryption and encryption as well. Base coding and algorithms are easy to implement. Actually, it's not usually used for encoding, but at sometimes it appears to be like encoding. Base algorithms convert the character or phrase to a fixed length of character to make the transfer of data more secure. Cryptography is defined as the method that cipher information, depending on particular algorithms and codes make the info unreadable to the human eyes unless it is decrypted back by the codes that were pre decided by the client/sender. The cryptographic algorithms needed to be improved to make the data integrity and security level increase.

REFERENCES

[1] J. Liu et al., "A Comprehensive Privacy-Preserving Federated Learning Scheme with Secure Authentication and Aggregation for Internet of Medical Things," in IEEE Journal of Biomedical and Health Informatics, doi: 10.1109/JBHI.2023.3304361.

[2] Ramisetty, Sowjanya; Anand, Divya; Kavita; Verma, Sahil; Jhanjhi, N. Z.; Masud, Mehedi; Baz, Mohammed, Computer Systems Science and Engineering 2023, 45(2), 1971-1983.
https://doi.org/10.32604/csse.2022.021924

[3] Kaur, Ramanpreet, Divya Anand, Upinder Kaur, Sahil Verma, Kavita, Seok-Wook Park, A. S. M. Sanwar Hosen, and In-Ho Ra. 2023.

"An Advanced Job Scheduling Algorithmic Architecture to Reduce Energy Consumption and CO2 Emissions in Multi-Cloud" Electronics 12, no. 8: 1810. https://doi.org/10.3390/electronics12081810

[4] Upadhyay, Shrikant, Mohit Kumar, Aditi Upadhyay, Sahil Verma, Kavita, A. S. M. Sanwar Hosen, In-Ho Ra, Maninder Kaur, and Satnam Singh. 2023. "Digital Image Identification and Verification Using Maximum and Preliminary Score Approach with Watermarking for Security and Validation Enhancement" Electronics 12, no. 7: 1609. https://doi.org/10.3390/electronics120716090 . O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, RF and Microwave.

[5] Bahuguna, A., Ashraf, A., Kavita, Verma, S., Negi, P. (2023). Brain Tumor Classification from MRI Scans. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 537. Springer, Singapore. https://doi.org/10.1007/978-981-99-3010-4_57

[6] Gupta, H., Kaur, A., Kavita, Verma, S., Rawat, P. (2023). Recognition of Handwritten Digits Using Convolutional Neural Network in Python and Comparison of Performance for Various Hidden Layers. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 537. Springer, Singapore. https://doi.org/10.1007/978-981-99-3010-4_58

[7] Dhetarwal, M., Ashraf, A., Verma, S., Kavita, Rawat, B. (2023). Employee Turnover Prediction Using Machine Learning. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 537. Springer, Singapore. https://doi.org/10.1007/978-981-99-3010-4_55

[8] Thind, R., Divya, K., Verma, S., Kavita, Kaur, N., Uniyal, V. (2023). Voice Email for the Visually Disabled. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 537. Springer, Singapore. https://doi.org/10.1007/978-981-99-3010-4_60

[9] Jain, Shikha, Navneet Kaur, Sahil Verma, Kavita, A. S. M. Sanwar Hosen, and Satbir S Sehgal. 2022. "Use of Machine Learning in Air Pollution Research: A Bibliographic Perspective" Electronics 11, no. 21: 3621. https://doi.org/10.3390/electronics11213621D . Krishnamoorthy and S. Chidambaranathan.

[10] N. Varol, F. Aydog˘an, and A. Varol, "Cyber Attacks Targeting Android Cellphones," The 5th International Symposium on.

[11] S. Tayal, N. Gupta, P. Gupta, D. Goyal, and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 763–770, 2017.

[12] I. A. Shah, Q. Sial, N. Z. Jhanjhi, and L. Gaur, "The Role of the IoT and Digital Twin in the Healthcare Digitalization Process: IoT and Digital Twin in the Healthcare Digitalization Process," Digital Twins and Healthcare: Trends, Techniques, and Challenges, pp. 20–34, 2023.

[13] N. Z. Jhanjhi, S. N. Brohi, N. A. Malik, and M. Humayun, "Proposing a hybrid rpl protocol for rankand wormhole attack mitigation using machine learning," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), pp. 1–6, 2020.

[14] K. Hussain, S. J. Hussain, N. Jhanjhi, and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," in 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–4.

[15] I. A. Shah, Q. Sial, N. Z. Jhanjhi, and L. Gaur, "Use Cases for Digital Twin," Digital Twins and Healthcare: Trends, Techniques, and Challenges, pp. 102–118, 2023.

[16] S. Vanangamudi, S. Prabhakar, C. Thamotharan, and R. Anbazhagan.

[17] V. Khanaa, K. Mohanta, and T. Saravanan, "Performance analysis of FTTH using GEPON in direct and external modulation," Indian Journal of Science and Technology, vol. 6, pp. 4848–4852, 2013.

[18] K. P. Thooyamani, V. Khanaa, and R. Udayakumar, "Virtual instrumen- tation based process of agriculture by automation," Middle - East Journal of Scientific Research, vol. 20, pp. 2604–2612, 2014.

[19] R. Agarwal, and A. G. Thomas, "Performance comparison of deep cnn models for detecting driver's distraction," Materials & Continua, vol. 68, no. 3, pp. 4109–4124, 2021.

[20] A. Almusaylim, Z. Jhanjhi, N. Z. Alhumam, and A, "Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP," Sensors, vol. 20, no. 21, pp. 5997–5997, 2020.

[21] A. Hussain, "A Resource Efficient hybrid Proxy Mobile IPv6 extension for Next Generation IoT Networks," IEEE Internet of Things Journal.

[22] I. Batra, "Hybrid Logical Security Framework for Privacy Preservation in the Green Internet of Things," Sustainability, vol. 12, pp. 5542–5542, 2020.

[23] S. More, "Security Assured CNN-Based Model for Reconstruction of Medical Images on the Internet of Healthcare Things," IEEE Access, vol. 8, pp. 126 333–126 346, 2020.

[24] V. Singhal, "Artificial Intelligence Enabled Road Vehicle-Train Collision Risk Assessment Framework for Unmanned Railway Level Crossings," IEEE Access, vol. 8, pp. 113 790–113 806, 2020.

[25] M. Arora, "A Systematic Literature Review of Machine Learning Esti- mation Approaches in Scrum Projects," in Cognitive Informatics and Soft Computing. Advances in Intelligent Systems and Computing, Mallick, P., Balas, V., Bhoi, A., Chae, and GS., Eds., vol. 1040. Springer, 2020.

[26] M. Kumar, P. Mukherjee, K. Verma, S. Verma, and D. B. Rawat, "Improved Deep Convolutional Neural Network based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks," IEEE Transactions on Network Science and Engineering.

[27] M. Kaur, "Flying Ad-Hoc Network (FANET): Challenges and Routing Protocols," Journal of Computational and Theoretical Nanoscience, vol. 17, no. 6, pp. 2575–2581, 2020.

[28] Mahmoud A. Zaher , Nabil M. Eldakhly, Brain Storm Optimization with Long Short Term Memory Enabled Phishing Webpage Classification for Cybersecurity, Journal of Cybersecurity and Information Management, Vol. 9 , No. 2 , (2022) : 20-30 (Doi : https://doi.org/10.54216/JCIM.090202)

[29] Lobna Osman, An Intelligent Spatial Military Intrusion Detection using Reactive Mobility Unmanned Vehicles Based on IoT and metaheuristic Optimization Algorithm, Journal of Cybersecurity and Information Management, Vol. 9 , No. 2 , (2022) : 31-41 (Doi : https://doi.org/10.54216/JCIM.090203)

[30] Mohammed. I. Alghamdi , Abeer. Y. Salawi , Salwa. H. Alghamdi, Smart Model for Securing Software Defined Networks, Journal of Cybersecurity and Information Management, Vol. 10 , No. 1 , (2022) : 08-17 (Doi : https://doi.org/10.54216/JCIM.0100101)

[31] Marwa M. Eid , M. I. Fath Allah, Detection and Classification of Malware Using Guided Whale Optimization Algorithm for Voting Ensemble, Journal of Cybersecurity and Information Management, Vol. 10 , No. 1 , (2022) : 34-42 (Doi : https://doi.org/10.54216/JCIM.100102)

[32] Shereen H. Ali, A Novel Intrusion Detection Framework (IDF) using Machine Learning Methods, Journal of Cybersecurity and Information Management, Vol. 10 , No. 1 , (2022) : 43-54 (Doi : https://doi.org/10.54216/JCIM.100103)

[33] Marwa M. Eid , Shaimaa A. Hussien, An Enhanced Hybrid Chaotic Technique for Protecting Medical Images, Journal of Cybersecurity and Information Management,

Vol. 10 , No. 1 , (2022) : 55-68 (Doi : https://doi.org/10.54216/JCIM.100104)

[34] Faisal A. Garba , Rosemary M. Dima , A. Balarabe Isa , A. Abdulrazaq Bello , A. Sarki Aliyu , F. Umar Yarima , S. Abbas Ibrahim, Re-Evaluating the Necessity of Third-Party Antivirus Software on Windows Operating System, Journal of Cybersecurity and Information Management, Vol. 10 , No. 1 , (2022) : 18-33 (Doi : https://doi.org/10.54216/JCIM.090105).

[35] Adeyemo, V. E., Abdullah, A., JhanJhi, N. Z., Supramaniam, M., & Balogun, A. O. (2019). Ensemble and deep-learning methods for two-class and multi-attack anomaly intrusion detection: an empirical study. International Journal of Advanced Computer Science and Applications, 10(9).

[36] Sennan, S., Somula, R., Luhach, A. K., Deverajan, G. G., Alnumay, W., Jhanjhi, N. Z., ... & Sharma, P. (2021). Energy efficient optimal parent selection based routing protocol for Internet of Things using firefly optimization algorithm. Transactions on Emerging Telecommunications Technologies, 32(8), e4171.