Analysis of design goals of cryptography algorithms based on different components

Ali Mohammad Norouzzadeh Gil Molk[1], Mohammad Reza Aref [2], Reza Ramazani Khorshiddoust[3]
[1]Department of Computer Engineering, Islamic Azad University, North Tehran Branch, Tehran, Iran
[2]Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
[3]Department of Industrial Engineering & Management Systems, Amirkabir University of Technology, Tehran, Iran

Article Info

Article history:

Received Feb 8, 2021
Revised Apr 20, 2021
Accepted May 1, 2021

Keywords:

Analysis
Component
Cryptography algorithms
IoT
Telemedicine

ABSTRACT

Cryptography algorithms are a fundamental part of a cryptographic system that is designed and implemented to increase information security. They are the center of attention of experts in the information technology domains. Although the cryptography algorithms are implemented to attain the goals such as confidentially, integrity, and authenticity of designing, but other matters that must be noticed by designers include speed, resource consumption, reliability, flexibility, usage type, and so on. For the useful allocation of hardware, software, and human resources, it is important to identify the role of each of the factors influencing the design of cryptographic algorithms to invest in the development of cryptographic knowledge. This paper examines 1700 papers, documents, and technical reports of international journals in the specific lengthy period (1978-2019), and the goal of the design and implementation of cryptography algorithms in a different period is extracted. Using a statistical population that consists of time and the number of documents in a long time and also a variety of data, leads this study to have a reliable result and attract the attention of designers. The results show that in recent years, attention to new usage such as IoT and telemedicine, as well as lightweight cryptography, has increased to achieve the main goals.

Corresponding Author:

Mohammad Reza Aref
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
Email: aref@sharif.edu

1. INTRODUCTION

According to Kenneth Geers, a cybersecurity strategist, the predominant aspect of national security in 2025 depends on the development of information technology [1]. On the other hand, cryptography is the most critical mechanism for upgrading the security level of information. Every cryptography system includes three parts: cryptography algorithms, cryptography keys, and security protocols. Moreover, cryptography algorithms are a fundamental part of this system [2]. However, cryptography algorithms are implemented to attain the goals such as security or confidentiality, integrity, and authenticity of designing [3], but for designing them, many components should be considered, such as speed, resource consumption, usage type [4]-[6]. So, providing all of these needs in algorithm design simultaneously is a problematic matter and, in some cases, is impossible. If contradictory goals are considered in defining the goals of designing an algorithm, most algorithms can be broken, and if the attacker has enough time, resources and desire, it can expose the information [7].

The strength of cryptography highly depends on the design and implementation of cryptography algorithms [8], and the theoretical properties of algorithms depend on the validity and integrity of their implementation in software and hardware [9]. On the other hand, there are many challenges for implementing cryptography algorithms such as runtime, memory usage and computing power consumption, which are all of the mentioned factors that impact the goals for designing the algorithm [10].

In [11] the general tendency towards cryptography in various sectors of the industry has been studied in a 13-year period (2005-2018), which shows that in 2005, 15% of organizations and in 2017, 43% of them have a cryptographic strategy. It can be said that today, the most significant features of cryptography are system function and delay time, policy implementation and support for cloud deployment and IoT cryptography [12]-[15]. As can be seen, the new necessities in this domain, such as quantum cryptography [16] and smart grid [17], require these needs to be considered in the design of cryptographic algorithms. So the purpose of this study is examination and statistical analysis of goals of design and implementation of cryptography algorithms based on different components [18].

There have been studies to compare cryptographic algorithms from different points of view such as security of online applications through cryptographic algorithms [19], data and applications security and privacy [20], [21], increasing security in software development [22] and lightweight algorithms in IoT applications [23]-[26]. In this paper, the approach of cryptographic algorithm designers at various times in terms of several components, such as security, speed, simplicity, flexibility, usability, and resource usage, will be analyzed.

2. METHODOLOGY

In order to accurately and reliably examine the goals, methods, and mechanisms of designing and implementing cryptographic algorithms, comprehensive information is needed in terms of the time interval, type of algorithm (symmetric, asymmetric, and Hash functions), and type of applications. There are several methods to obtain valid data to determine the value of each index, the most important of which are: own use, experiments & tests, simulations, observations, dialogues, structure interviews, and questionnaires [27]. Figure 1 shows the reliability of each of these methods, and in this paper, the observations method is used.

In this regard, we tried to use different sources over a relatively long period of time, from 1978 to 2019. The reason for this is the existence of essential principles in the design of cryptographic algorithms that are still used over time. Finally, Google Scholar was chosen as a tool that provides beneficial statistical information in the field of various sciences, including cryptography. The keywords «cryptography algorithm» and «cryptographic algorithm» were used to extract valid papers and reports from this database. The initial criterion for selecting papers with the above keywords was the minimum number of citations to that paper or report. Depending on the year of publication, the minimum number of citations varied according to Table 1.

After reviewing the content of 1742 papers and extracted reports, in the next step, 863 items that were directly related to the design of cryptographic algorithms were selected and used. Their frequency in terms of publication in reputable sources is shown in Figure 2. As can be seen, 62% of the papers used with the specified number of citations in Table 1 have been published in four authoritative scientific references: IEEE (30%), Springer (17%), Elsevier (13%), and ACM (2%). Other documents and reports were extracted from reputable sources such as NIST, ITU, as well as international competitions such as ECRYPT.

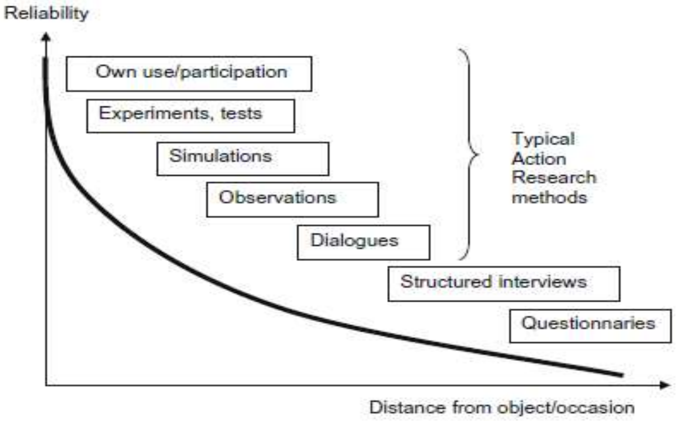


Figure 1. Reliability, depending on the investigation method used [27]

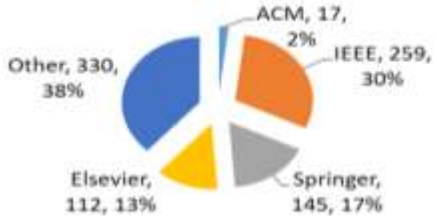


Figure 2. Percentage of considering published papers in various journals

Table 1. Number of papers, publication year, and number of times of citations

Year	Number	Citation	Year	Number	Citation	Year	Number	Citation	Year	Number	Citation
1978-1999	28	23	2005	55	30	2011	144	10	2017	88	7
2000	47	20	2006	66	30	2012	163	10	2018	71	5
2001	54	30	2007	66	30	2013	154	10	2019	63	5
2002	57	30	2008	48	30	2014	134	13			
2003	61	30	2009	71	30	2015	112	10			
2004	54	30	2010	73	30	2016	133	10			

3. EXTRACTION OF COMPONENTS

3.1. The purposes of designing cryptographic algorithms

One of the most essential components in design and implementation of cryptographic algorithms is the goal/goals of designers of its implementation. The trend towards cryptography in new applications such as cloud computing, IoT, and resource-constrained devices requires that in designing and implementing cryptographic algorithms, many new necessities should be considered. To achieve this, by reviewing the selected sources, 12 general goals for designing cryptographic algorithms were extracted. Different types of extracted goals and their frequency are shown in Table 2. Obviously, in most cases, the necessity of designing an algorithm is to achieve several goals simultaneously. For example, the purpose of designing an algorithm could be to achieve high speed, adequate security, and high flexibility using various techniques such as Self-stabilizing techniques [28], [29], CNN method [30], [31], image and signal processing [32]-[34], hybrid methods [15] and so on, at the same time.

As can be seen, the security component with 516 items has the highest repetition among other goals, which indicates that the primary purpose of designing the encryption algorithm was to increase security, which is obvious. Usability and speed goals are in second and third place after security. In other words, the biggest concern of algorithm designers is to increase the security of cryptographic algorithms based on their specific uses and also to increase speed. Figure 3 shows the frequency of each target in the selected statistical population.

By using the dimension reduction technique [35]-[37], the total number of components (goals) is reduced to 8 components. In this regard, we remove some of them in the way:

a. Since the cost in designing the algorithm includes computational overhead, bandwidth, CPU usage, memory usage, and occupation level in hardware cryptography, and all of these indicators are seen in resource usage, so the “cost reduction” component is integrated into the “resource usage” component.
b. Since improving image quality and performance is to increase performance, these two components are integrated into the performance component.
c. Since the primary purpose of all algorithms is to increase performance by reducing resource consumption, ease of implementation and increasing speed, security, reliability, flexibility, and scalability, by reviewing related papers (36 papers), all of them were merged into the above-mentioned components based on the explicitness of the text, except for six papers.

Table 2. Goal of cryptography algorithm design and their frequency

Goal	Frequency	Goal	Frequency	Goal	Frequency
Security	516	Flexibility	45	Speed	247
Use of Resource	91	Scalability	22	Reliability	11
Decrease Cost	9	Performance	36	Usability	337
Simplicity	38	Image Quality	9	Function Improving	1

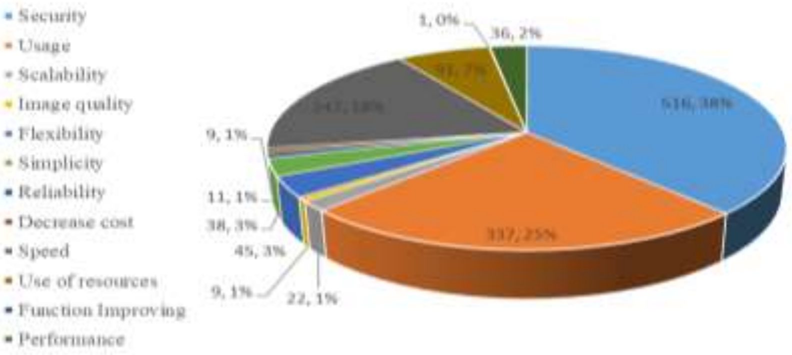


Figure 3. Percentage of the goal of cryptography algorithm design

Finally, from the remaining 814 papers, documents, and technical reports, eight main objectives for the design of cryptographic algorithms were extracted. Table 3 shows these objectives and their frequency and frequency percentage in a total of 814 papers. The number and percentage of eight goals at different time intervals are shown in Table 4 and its chart in Figure 4.

Table 3. Eight goals of cryptography algorithms design and their percentage of frequency

Row	Index Name	Number	Percentage	Row	Index Name	Number	Percentage
1	Security	516	63.4	5	Flexibility	45	5.5
2	Optimum use of resources	81	10	6	Scalability	22	2.7
3	Usability	338	41.5	7	Speed	247	30.3
4	Simplicity	38	4.7	8	Reliability	11	1.4

Table 4. Numbers and percentage of eight goals of encryption algorithm design in different period of time

Years	Total	Security		Usability		Speed		Resource		Flexibility		Simplicity		Scalability		Reliability	
	#	#	%	#	%	#	%	#	%	#	%	#	%	#	%	#	%
1978-2000	31	14	45.16	12	38.71	12	38.71	2	6.45	5	16.13	4	12.9	2	6.45	1	3.23
2001-2005	121	67	55.37	33	27.27	50	41.32	12	9.92	7	5.79	2	1.65	5	4.13	1	0.83
2006-2010	145	88	60.69	65	44.83	39	26.9	15	10.34	16	11.03	5	3.45	7	4.83	1	0.69
2011-2015	316	203	64.24	132	41.77	86	27.22	33	10.44	11	3.48	17	5.38	6	1.9	6	1.9
2016-2019	201	144	71.64	96	47.76	99	29.85	19	9.45	6	2.99	10	4.98	2	0.99	2	0.99

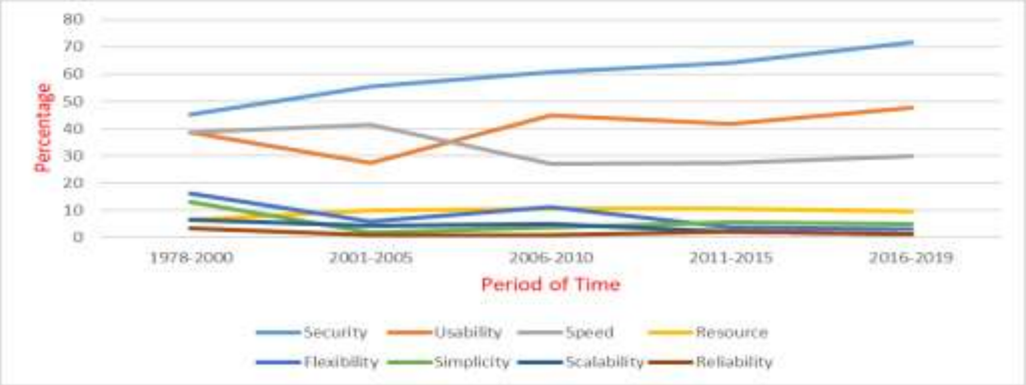


Figure 4. Diagram of the percentage of the state of goals of cryptography algorithm design in a period of time

As can be seen, the three main goals of algorithm designers that are far ahead of other goals are security, usability, and speed. Security, which is the most crucial goal in cryptography, has always been growing, and other goals have changed as needed. Since 2005, the usability goal has received more attention.

Obviously, with the emergence of new uses, designing and implementing algorithms based on new hardware and software conditions is one of the most critical challenges for designers. For example, with the advent of IoT, which is inherently vulnerable to a variety of security threats [38], [39], due to its application in various fields of health [40], agriculture [41], industry [42] and so on, there is a risk of information leakage, or it could damage the economy if the necessary security measures are not taken [43], [44]. Such threats may be considered as one of the most important obstacles to the development of IoT [45], [46]. It is also observed that the optimal use of resources has received more attention over time [47], [48], and this is due to the development of wireless networks with limited resources, the Internet of Things, and the increasing use of sensors.

The internet initially consisted of only a small cloud with only a few interconnected networks. At the time, all that was done for routing was to define the nodes of these finite networks and make connections between them. But the Internet has not remained small, and a greater combination of networks has emerged on the Internet, which requires a dynamic routing system to communicate. As a result, a new external routing protocol was defined that provided scalability capabilities. The scalability of the BGP protocol allowed it to perform such routing well, although security and data protection is of high significance [49]-[52].

Another issue is the simultaneous consideration of two main goals in the design of cryptographic algorithms. According to Table 5, the two goals of usability and security have the most in common. The two goals of security and speed are in second place, and the two goals of usability and speed are in third place, and usability and resources are in the fourth place. The diagram of the two-by-two important goals of security, speed, usability, and use of resources at different time intervals is shown in Figure 5.

Table 5. Frequency of goals in a mutual way

	Security	Simplicity	Reliability	Scalability	Use of Resource	Flexibility	Speed	Usability
Security	-	23	7	5	17	14	85	205
Simplicity	23	-	1	1	5	4	8	13
Reliability	7	1	-	0	0	1	3	3
Scalability	5	1	0	-	1	5	5	5
Use of Resource	17	5	0	0	-	7	34	41
Flexibility	14	4	1	5	7	-	16	15
Speed	85	8	3	5	34	16	-	73
Usability	204	13	3	5	41	15	73	0

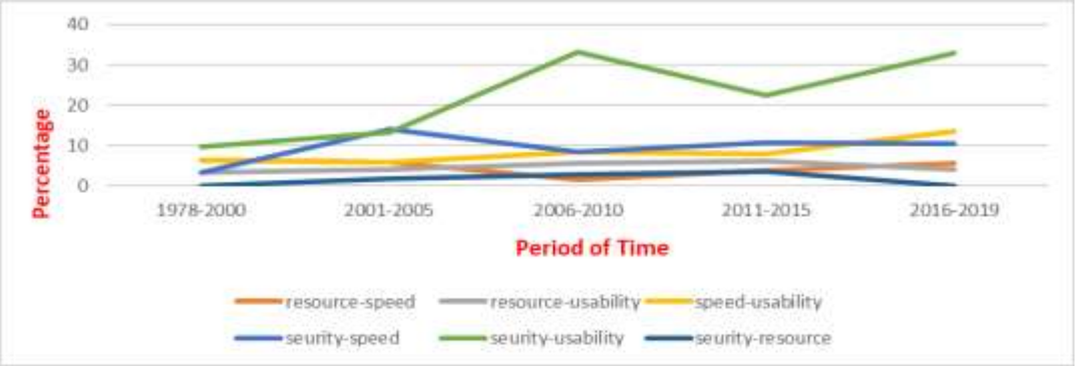


Figure 5. Diagram of the percentage of the goals the security-speed and use -optimum use of resource in case of sharing pairwise

As can be seen, the two speed-usability goals have grown steadily since 2015. The reason for this is the emergence of new uses, especially mobile usability, and the increase in the speed of applications and communication networks. The lag of the cryptography speed leads to less use of it and ultimately increases insecurity. Because of this, speed has been one of the most important goals in recent years. The uniform growth of optimum use of resources - speed is in the same direction. The increasing use of mobile networks and types of equipment that have limited resources has caused these two common goals to attract more attention from designers of cryptographic algorithms in recent years. Between 2010 and 2015, shared goals of security-usability have decreased, and security speed has increased. The most important reason is the increase in the speed of communication networks and, consequently, applications that increase the need for high-speed use.

3.2. Usage of cryptographic algorithms

Regarding the use of cryptographic algorithms, 18 different uses were extracted from the existing statistical community, of which multimedia use with 163 repetitions is the most practical goal of cryptographic algorithm designers. Figure 6 shows the types of uses with their frequency in the existing statistical community. As can be seen, the first seven uses are applications in multimedia environments, wireless networks, cloud environments, limited resources, IoT, medical uses, and real-time applications. The graph of the status of these seven significant uses at different time intervals is shown in Figure 7. It is noteworthy that cryptographic algorithm designers have considered the use of the cloud environment for cryptographic algorithms since 2010 and IoT since 2012. Also, since 2015, multimedia uses, IoT, and medical applications have been on the rise. Due to IoT in medicine and the sensitivity of medical information confidentiality, one of the most critical concerns of cryptographic algorithm designers today is the design of algorithms for encrypting medical information [53]-[56].

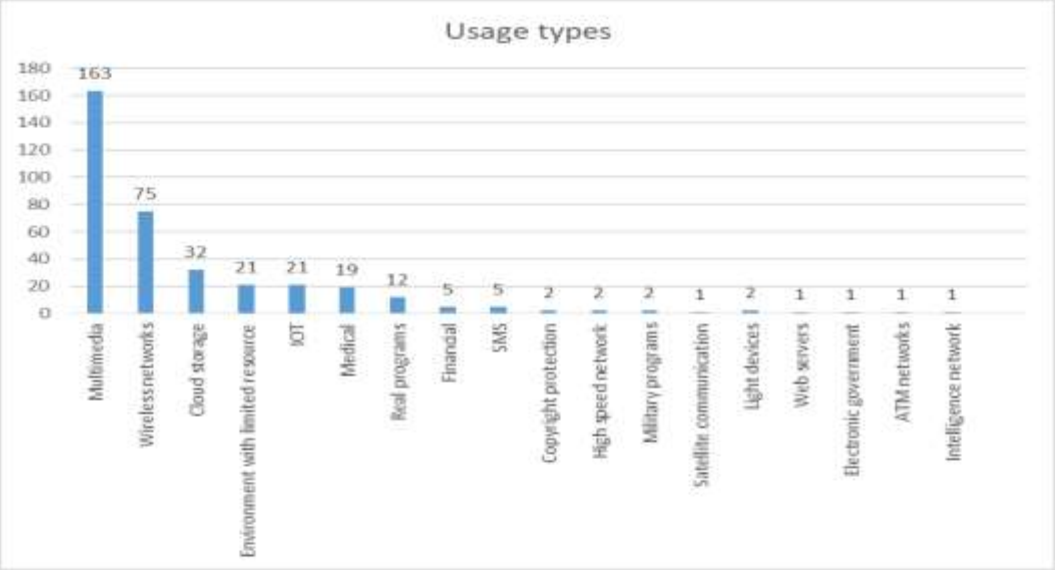


Figure 6. Frequency of different cryptography algorithms design usage

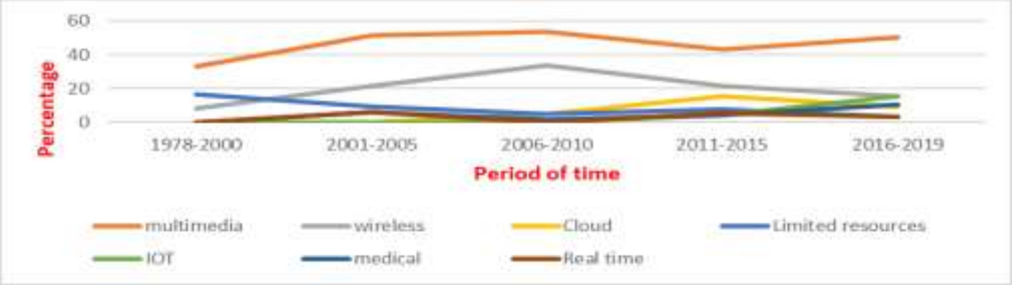
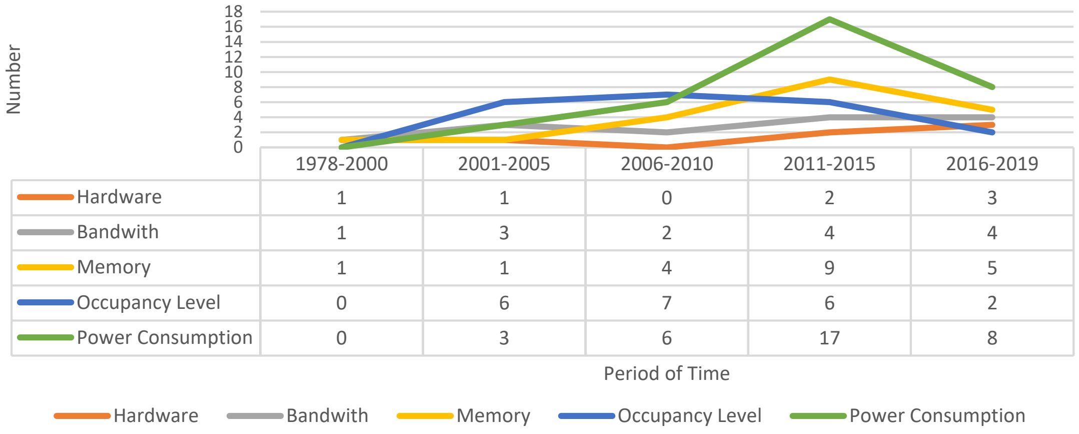


Figure 7. Diagram of the primary uses of different cryptography algorithms design

3.3. Optimal use of resources

Another critical goal of cryptographic algorithm designers is to design an algorithm that uses fewer resources after implementation and at runtime. According to a study conducted in this statistical community, the essential sources considered by cryptographic algorithm designers are hardware, memory, bandwidth, power consumption, and occupancy level. The percentage of each of the above sources in the design of cryptographic algorithms is shown in Figure 8.

As can be seen, since 2005, the two sources of memory and hardware have been on the rise and have received more attention. According to the diagram in Figure 8, energy consumption is more considered by algorithm designers. One of the most important reasons for increasing IoT security is that they are very vulnerable to attacks [57]. Also, due to the wireless communication environment, limited power resources, and low computability, the implementation of conventional security algorithms will lead to obstacles in their performance [58]. This suggests that in the future, the use of resources as an important factor in the design of cryptographic algorithms should be seriously considered.



	1978-2000	2001-2005	2006-2010	2011-2015	2016-2019
Hardware	1	1	0	2	3
Bandwith	1	3	2	4	4
Memory	1	1	4	9	5
Occupancy Level	0	6	7	6	2
Power Consumption	0	3	6	17	8

Figure 8. Diagram of the percentage of the different resources of cryptography algorithm design

4. CONCLUSION

In this research, by reviewing more than 1700 papers, technical reports, and documents published by international organizations for the design and implementation of cryptographic algorithms, it was concluded that the main goals of designers in order of their priority are increasing security, attention to use, increasing speed and optimal use of resources, simplicity, increasing flexibility, scalability, and reliability. Regarding the optimal use of resources, due to the advancement of technology and the emergence of communication networks with new features, the resources considered based on priority are power consumption, lower occupancy level, memory usage, bandwidth usage, and hardware usage. According to the given statistics in this paper, due to the new needs of users in various fields, several uses of these cryptographic algorithms that designers consider in order of priority are multimedia uses, wireless networks, cloud computing, environment with limited resources, IoT, medical use, and real-time applications. Therefore, to design new cryptographic algorithms, primary goals and technical requirements must be considered. The desired algorithm must be designed and implemented based on these so that in addition to the management of required hardware and software resources, they can have more flexibility in new applications.

REFERENCES

[1] L. J. Fennelly, M. Beaudry, and M. A. Perry, *Security in 2025*, ASIS International, 2017.

[2] P. Kocher, R. Lee, G. McGraw, A. Raghunathan, and S. Ravi, “Security as a new dimension in embedded system design,” in *Proc. - Des. Autom. Conf.*, 2004, pp. 753-760, doi: 10.1145/996566.996771.

[3] Sourabh Bhat, and Vivek Kapoor “Secure and efficient data privacy, authentication and integrity schemes using hybrid cryptography,” in *Kamal R., Henshaw M., Nair P. (eds) International Conference on Advanced Computing Networking and Informatics. Advances in Intelligent Systems and Computing*, vol 870. Springer, Singapore, doi: 10.1007/978-981-13-2673-8_30.

[4] O. G. Abood, and S. K. Guirguis, “A survey on cryptography algorithms,” *Int. J. Sci. Res. Publ.*, vol. 8, no. 7, Jul. 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.

[5] A. Kumar Gupta, P. Mathur, and P. Vashishtha, “Comparative study of cryptography for cloud computing for data security,” *Recent Adv. Comput. Sci. Commun.*, vol. 12, pp. 1-1, 2019, doi: 10.2174/2666255813666190911114909.

[6] K. B. Logunleko, O. D. Adeniji, A. Logunleko, and O. State, “A comparative study of symmetric cryptography mechanism on DES , AES and EB64 for information security,” vol. 8, no. February, pp. 45-51, 2020.

[7] A. A. Soofi, I. Riaz, and U. Rasheed, “An enhanced vigenere cipher for data security,” *Int. J. Sci. Technol. Res.*, vol. 4, no. 8, pp. 141-145, 2015.

[8] D. Nilesh, and M. Nagle, “The new cryptography algorithm with high throughput,” in *2014 Int. Conf. Comput. Commun. Informatics Ushering Technol. Tomorrow, Today, ICCCI 2014*, 2014, pp. 3-7, doi: 10.1109/ICCCI.2014.6921739.

[9] A. Vassilev, L. Feldman, and G. Witte, “Automated cryptographic validation (ACV) testing,” in *ITL bulletin for September 2018*, pp. 1-4, 2018.

[10] M. Nagendra, and M. Chandra Sekhar, “Performance improvement of advanced encryption algorithm using parallel computation,” *Int. J. Softw. Eng. its Appl.*, vol. 8, no. 2, pp. 287-296, 2014, doi: 10.14257/ijseia.2014.8.2.28.

[11] Thales, *Global encryption trends study*, Ponemon Institute Research, 2018. .

[12] Y. Choi, “Cryptanalysis on privacy-aware two-factor authentication protocol for wireless sensor networks,” *Int. J. Electr. Comput. Eng.*, vol. 8, no. 1, pp. 605-610, 2018, doi: 10.11591/ijece.v8i1.pp605-610.

[13] M. A. A. K. Al-Dabbas, A. Alabaichi, and A. S. Abbas, “Dual method cryptography image by two force secure and steganography secret message in IoT,” *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 18, no. 6, pp. 2928-2938, 2020, doi: 10.12928/TELKOMNIKA.v18i6.15847.

[14] R. F. Abdel-Kader, S. H. El-Sherif, and R. Y. Rizk, “Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3295-3306, 2020, doi: 10.11591/ijece.v10i3.pp3295-3306.

[15] P. Siva Sankaran, and V. B. Kirubanand, “Hybrid cryptography security in public cloud using TwoFish and ECC algorithm,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 4, pp. 2578-2584, 2019, doi: 10.11591/ijece.v9i4.pp2578-2584.

[16] B. Muruganantham, P. Shamili, S. Ganesh Kumar, and A. Murugan, “Quantum cryptography for secured communication networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 407-414, 2020, doi: 10.11591/ijece.v10i1.pp407-414.

[17] S. M. S. Reza *et al.*, “Salsa20 based lightweight security scheme for smart meter communication in smart grid,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)* vol. 18, no. 1, pp. 228–233, 2020, doi: 10.12928/TELKOMNIKA.V18I1.14798.

[18] J. Zalewski, A. J. Kornecki, B. D. Czejdo, F. G. Gonzalez, N. Subramanian, and D. Trawczynski, “Curriculum development for embedded systems security,” in *2014 ASEE Annual Conference & Exposition, Indianapolis, Indiana*, doi: 10.18260/1-2--20237.

[19] A. Sharma, “Comparative study of symmetric cryptography algorithm,” thesis Faculty of Engineering, Department of Computer Science & Engineering, Pacific University (PAHER), Udaipur (Rajasthan), 2014. [Online]. Available: https://www.researchgate.net/publication/286863418_comparative_study_of_symmetric_cryptography_algorithm, doi: 10.13140/RG.2.1.1031.5601.

[20] Layla Pournajaf, Farnaz Tahmasebian, Li Xiong, Vaidy Sunderam, and Cyrus Shahabi, “Privacy preserving reverse k-Nearest Neighbor queries,” In *2018 19th IEEE International Conference on Mobile Data Management (MDM),* 2018, doi: 10.1109/MDM.2018.00035.

[21] Farnaz Tahmasebian, Li Xiong, Mani Sotoodeh, and Vaidy Sunderam, “Crowdsourcing under data poisoning attacks: A comparative study,” In *IFIP Annual Conference on Data and Applications Security and Privacy*, Spinger, 2020, pp. 310-332, doi: 10.1007/978-3-030-49669-2_18.

[22] Balavivekanandhan, A., “A comparative study of cryptography algorithm in data security for software,” *Journal of the Gujarat Research Society*, 2019, vol. 21, pp. 1904–1918.

[23] Navid Abapour, Aynaz Shafiesabet, and Rasoul Mahboub, “A novel security based routing method using ant colony optimization algorithms and RPL protocol in the IoT networks,” *Mapta Journal of Electrical and Computer Engineering (MJECE)*, vol. 3, no. 1, pp. 1-9, 2021.

[24] D. Sehrawat, N. S. Gill, and M. Devi, “Comparative analysis of lightweight block ciphers in IoT-enabled smart environment,” in *2019 6th International Conference on Signal Processing and Integrated Networks, SPIN 2019*, pp. 915-920, May 2019, doi: 10.1109/SPIN.2019.8711697.

[25] T. Omrani, R. Rhouma, and L. Sliman. “Lightweight cryptography for resource-constrained devices: A comparative study and rectangle cryptanalysis,” in Lecture Notes in Business Information Processing, 2018, vol. 325, pp. 107-118, doi: 10.1007/978-3-319-97749-2_8.

[26] S. Kaur, and S. Kaur, “Comparative analysis of lightweight cryptography algorithms for smart grids,” in *4th IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2017*, Sep. 2017, vol. 2017-January, pp. 564-567, doi: 10.1109/ISPCC.2017.8269742.

[27] S. Ottosson, *Developing and Managing Innovation in a Fast Changing and Complex World*, Springer International Publishing, 2019, doi: 10.1007/978-3-319-94045-8.

[28] Ramtin A., Hakami V., Dehghan M., “A perturbation-proof self-stabilizing algorithm for constructing virtual backbones in wireless Ad-Hoc networks,” in *International Symposium on Computer Networks and Distributed Systems,* Computer Networks and Distributed Systems (CNDS 2013), Communications in Computer and Information Science, 2014, vol. 428, Springer, Cham, doi: 10.1007/978-3-319-10903-9_6.

[29] Amirreza Ramtin, Vesal Hakami, and Mehdi Dehghan, “A self-stabilizing clustering algorithm with fault-containment feature for wireless sensor networks,” In *7'th International Symposium on Telecommunications (IST'2014),* 2014, doi: 10.1109/ISTEL.2014.7000799.

[30] Ali Jahanshahi, Hadi Zamani Sabzi, Chester Lau, and Daniel Wong, “GPU-NEST: characterizing energy efficiency of multi-GPU inference servers,” *IEEE Computer Architecture Letters*, vol. 19, no. 2, pp. 139-142.

[31] Jahanshahi, A., “TinyCNN: A Tiny Modular CNN Accelerator for Embedded FPGA,” 2019, *arXiv:1911.06777*.

[32] Pourjabar, S., and Choi, G. S., “CVR: A Continuously Variable Rate LDPC Decoder Using Parity Check Extension for Minimum Latency,” *Journal of Signal Processing Systems*, pp. 1-8, 2020, doi: 10.1007/s11265-020-01597-0.

[33] H. A. H. Al Naffakh, R. Ghazali, N. K. El Abbadi, and A. N. Razzaq, “A review of human skin detection applications based on image processing,” *Bull. Electr. Eng. Informatics*, vol. 10, no. 1, pp. 129-137, 2021, doi: 10.11591/eei.v10i1.2497.

[34] M. Moussa, “An iterative algorithm for color space optimization on image segmentation,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 1, pp. 199-205, 2020, doi: 10.12928/TELKOMNIKA.V19I1.15122.

[35] N. V. Thoai, “Criteria and dimension reduction of linear multiple criteria optimization problems,” *J. Glob. Optim.*, vol. 52, no. 3, pp. 499-508, 2012, doi: 10.1007/s10898-011-9764-4.

[36] T. Gal, and H. Leberling, “Redundant objective functions in linear vector maximum problems and their determination,” *Eur. J. Oper. Res.*, vol. 1, no. 3, pp. 176-184, 1977, doi: 10.1016/0377-2217(77)90025-X.

[37] R. Zhang, T. Du, and S. Qu, “A principal component analysis algorithm based on dimension reduction window,” *IEEE Access*, vol. 6, pp. 63737-63747, 2018, doi: 10.1109/ACCESS.2018.2875270.

[38] E. Hodo *et al.*, “Threat analysis of IoT networks using artificial neural network intrusion detection system,” in *2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016*, 2016, pp. 4-8, doi: 10.1109/ISNCC.2016.7746067.

[39] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed security model and threat taxonomy for the Internet of Things (IoT),” *Commun. Comput. Inf. Sci.*, vol. 89 CCIS, pp. 420-429, 2010, doi: 10.1007/978-3-642-14478-3_42.

[40] A. Alkhayyat, A. A. Thabit, F. A. Al-Mayali, and Q. H. Abbasi, “WBSN in IoT health-based application: Toward delay and energy consumption minimization,” *J. Sensors*, vol. 2019, 2019, doi: 10.1155/2019/2508452.

[41] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. H. M. Aggoune, “Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk,” *IEEE Access*, vol. 7, pp. 129551-129583, 2019, doi: 10.1109/ACCESS.2019.2932609.

[42] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” *Internet of Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/j.iot.2019.100059.

[43] H. J. Ban, J. Choi, and N. Kang, “Fine-grained support of security services for resource constrained internet of things,” *Int. J. Distrib. Sens. Networks*, vol. 2016, 2016, doi: 10.1155/2016/7824686.

[44] Shujaat Khan, Mansoor Ebrahim, and Kafeel Ahmed Khan, “Performance evaluation of secure force symmetric key algorithm,” in *Proc. Int. Multi-Topic Conf.(IMTIC), Pakistan*, 2015, pp. 11-13.

[45] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787-2805, 2010, doi: 10.1016/j.comnet.2010.05.010.

[46] M. Ebrahim, S. Khan, and U. Khalid, “Security risk analysis in peer 2 peer system,” 2012, *arXiv:1404.5123*.

[47] R. Jyothi, and N. G. Cholli, “An efficient approach for secured communication in wireless sensor networks,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 1641-1647, 2020, doi: 10.11591/ijece.v10i2.pp1641-1647.

[48] M. N. Hieu, D. H. Ngoc, C. H. Ngoc, T. D. Phuong, and M. T. Cong, “New primitives of controlled elements F2/4 for block ciphers,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 5, pp. 5470-5478, 2020, doi: 10.11591/IJECE.V10I5.PP5470-5478.

[49] Fahimeh Arab, Mohsen Karimi, and Seyed Mostafa Safavi, “Analysis of QoS parameters for video traffic in homeplug AV standard using NS-3,” In *2016 Smart Grids Conference (SGC)*, doi: 10.1109/SGC.2016.7882949.

[50] Mohsen Karimi, Ali Jahanshahi, Abbas Mazloumi, and Hadi Zamani Sabzi, “Border gateway protocol anomaly detection using neural network,” in *2019 IEEE International Conference on Big Data (Big Data)*, 2020, pp. 6092-6094, doi: 10.1109/BigData47090.2019.9006201.

[51] Effy Raja Naru, Hemraj Saini, and Mukesh Sharma, “A recent review on lightweight cryptography in IoT,” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, doi: 10.1109/I-SMAC.2017.8058307.

[52] S. Deb, and M. M. Haque, “Elliptic curve and pseudo-inverse matrix based cryptosystem for wireless sensor networks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, p. 4479, 2019, doi: 10.11591/ijece.v9i5.pp4479-4492.

[53] B. K. Siddartha, and G. K. Ravikumar, “An efficient data masking for securing medical data using DNA encoding and chaotic system,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6008-6018, 2020, doi: 10.11591/ijece.v10i6.pp6008-6018.

[54] P. Aparna, and P. V. V. Kishore, “An efficient medical image watermarking technique in e-healthcare application using hybridization of compression and cryptography algorithm,” *J. Intell. Syst.*, vol. 27, no. 1, Jan. 2018, doi: 10.1515/jisys-2017-0266.

[55] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, “Hybrid optimization with cryptography encryption for medical image security in Internet of Things,” *Neural Comput. Appl.*, vol. 32, no. 15, pp. 10979-10993, Aug. 2020, doi: 10.1007/s00521-018-3801-x.

[56] P. T. Akkasaligar, and S. Biradar, “Selective medical image encryption using DNA cryptography,” *Information Security Journal*, vol. 29, no. 2, pp. 91-101, Mar. 03, 2020, doi: 10.1080/19393555.2020.1718248.

[57] M. A. Simplicio, M. V. M. Silva, R. C. A. Alves, and T. K. C. Shibata, “Lightweight and escrow-less authenticated key agreement for the internet of things,” *Comput. Commun.*, vol. 98, no. May, pp. 43-51, 2017, doi: 10.1016/j.comcom.2016.05.002.

[58] M. Usman, I. Ahmed, M. Imran, S. Khan, and U. Ali, “SIT: A lightweight encryption algorithm for secure internet of things,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, pp. 1-10, 2017, doi: 10.14569/ijacsa.2017.080151.