VOLUME V

ISBN No.: 978-81-953602-8-4

Computational Science

Estd. 1957

NALLAMUTHU GOUNDER MAHALINGAM COLLEGE

An Autonomous Institution, Affiliated to Bharathiar University, An ISO 9001:2015 Certified Institution,

Pollachi-642001

SUPPORTED BY

Riyasaa Labs

Sakthi as pure as mother's love

ABT Industries Ltd.,
Dairy Division

PROCEEDING

One day International Conference

EMERGING TRENDS IN SCIENCE AND TECHNOLOGY (ETIST-2021)

27th October 2021

Jointly Organized by

Department of Biological Science, Physical Science and Computational Science

NALLAMUTHU GOUNDER MAHALINGAM COLLEGE

An Autonomous Institution, Affiliated to Bharathiar University

An ISO 9001:2015 Certified Institution, Pollachi-642001.

Estd. 1957

Proceeding of the

One day International Conference on

EMERGING TRENDS IN SCIENCE AND TECHNOLOGY (ETIST-2021)

27th October 2021

Jointly Organized by

Department of Biological Science, Physical Science and Computational Science

ISBN No: 978-81-953602-8-4

978- 81- 953602- 8- 4

Nallamuthu Gounder Mahalingam College

An Autonomous Institution, Affiliated to Bharathiar University

An ISO 9001:2015 Certified Institution, 90 Palghat Road, Pollachi-642001.

www.ngmc.org

ABOUT THE INSTITUTION

A nations's growth is in proportion to education and intelligence spread among the masses. Having this idealistic vision, two great philanthropists late. S.P. Nallamuthu Gounder and Late. Arutchelver Padmabhushan Dr.N.Mahalingam formed an organization called Pollachi Kalvi Kazhagam, which started NGM College in 1957, to impart holistic education with an objective to cater to the higher educational needs of those who wish to aspire for excellence in knowledge and values. The College has achieved greater academic distinctions with the introduction of autonomous system from the academic year 1987-88. The college has been Re-Accredited by NAAC and it is ISO 9001 : 2015 Certified Institution. The total student strength is around 6000. Having celebrated its Diamond Jubilee in 2017, the college has blossomed into a premier Post-Graduate and Research Institution, offering 26 UG, 12 PG, 13 M.Phil and 10 Ph.D Programmes, apart from Diploma and Certificate Courses. The college has been ranked within Top 100 (72nd Rank) in India by NIRF 2021.

ABOUT CONFERENCE

The International conference on “Emerging Trends in Science and Technology (ETIST-2021)” is being jointly organized by Departments of Biological Science, Physical Science and Computational Science - Nallamuthu Gounder Mahalingam College, Pollachi along with ISTE, CSI, IETE, IEE & RIYASA LABS on 27th OCT 2021. The Conference will provide common platform for faculties, research scholars, industrialists to exchange and discus the innovative ideas and will promote to work in interdisciplinary mode.

EDITORIAL BOARD

LIST OF ARTICLES

Prevention of Cyber Attack Using Cloud IoT System

Dr. B. Azhagusundari[1] - Mrs. R. Latha[2]

ABSTRACT: Development in technology acts as a boom. Similarly, many hackers are starting to attack the network that increasing the cyber risk. Users and business organizations are highly affected due to the loss of data, corruption, and malware attack. Even they built a multi-level of security nothing seems to be possible to keep an endpoint for that. To compete with it new technologies and trends were embedded to overcome this situation. All this acts as the greatest hindrance to present society. To overcome these network attacks, there is a need for the replacement or collaboration of some modern new technological features and functionalities. That should be user-friendly as well it act as a bridge in fighting against malware and other types of attack. At this place the cloud computing in IOT does wonders. While building a highly secured protective wall using the Rivest Cipher 6 Advanced techniques while interacting that is interchanging the data using IoT, the user could reduce the cyber risk that is faced.

Keywords: Rivest Cipher 6 (RC6), Encrypt, Block Cipher, Decrypt, Internet of Things and Cloud Computing

1) Introduction

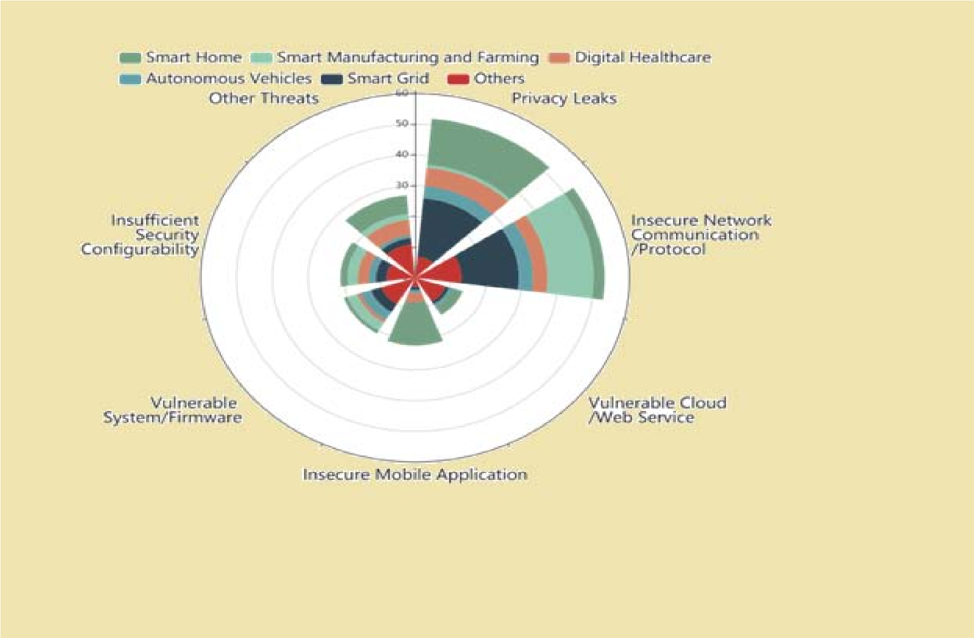
[1]In this pandemic situation, everyone switched towards dealing with online networks. People started showing interest in accessing their data and information online. At every office work from home concepts and techniques were encouraged for providing a high level of security for the employees. During processing, the data and information would be converted as a single file and it would be transferred for processing.[1] Since the people work from the different place and zones the main key concept that they use is data storage, data sharing, and processing. It gradually increases the cyber risk while processing and executing online. To sort out the problem the highly secured application is designed and using that the employees transfer their data and start working for the betterment of the project works. Here for adding an extra secured layer the advanced and enhanced [2]Rivest Cipher 6 algorithm has been effectively implemented. This algorithm mainly works as an encryption and decryption concept, where the data cannot be revealed by any external users. During the encryption process, it consists of 4 different w-bit and its registers. These registers are used for storing the data. The initial storage will be in plain text format that gets converted to the cipher. The data would get stored at that particular same register.[2] In end, a similar method of encryption techniques are followed for extracting that is encryption process. This technique supports reducing the loss of data, which acts as a great plus. It works out with the multidimensional key, where the concept of rework and fear about what would happen when data is hacked can be reduced. It keeps on processing simultaneously until the specific goal has been met.

Dr. B. Azhagusundari, Department of Computer Science, NGM College, Coimbatore, India.
Mrs. R. Latha, Department of Computer Science, Pollachi College of Arts and Science, Coimbatore, India.

2) Cause of Attack In 2021

The change in technology has created a great impact on the implementation and it starts enhancing out the human life. It simplifies the complex issues and lets the user meet all their need from the place where they are. That too the number of people who started using the technology increases multiple times during the Pandemic situation. The concept of work from home, online banking, online shopping, and online meeting was highly encouraged. In every business organization more than approximately 90% of the data has been shared online. That on other hand increases the risks and complexity of the issues. In the network, there are chances for the different types of attacks that create a risky cyber attack.

To overcome and to get rid of the issues new techniques and concepts came into existence. [3]The IoT has created a new paradigm where the network machine, as well as the device, is capable of improving the communication after collaborating to form the new process. The main reason for the cyber attack in IoT-based devices depends on the environmental monitoring, patient monitoring, logistics, and smart grids.[3][7]The security management concepts created a great flaw in the challenge due to its transient and dynamic nature that is established in connecting between two devices.[7] Now in this paper, the prediction of cyber attack that occurs at the networks are predicted and analyzed.



Threat Tags in Different Application Scenario

In the above prediction using [5,6]the sample research the vulnerable attack that arises due to the insecure network communication-based protocols increases gradually higher. There is a need for a multi-level security layer has been effectively applied for protecting the data while sharing through networks.[5,6]

2 a) Security in Cloud

During the storage process, there are lots of issues that arise in the backups, security of the data, file system, traffic, host security, and traffic. [4]In this proposed system there the RC6 algorithm techniques are used. The RC6 algorithm has four main components like the basic operation, key scheduling, Decryption techniques, and Encryption techniques.[4] It contains six main operations that are used for performing operations for integer addition, integer subtraction, bitwise exclusive, and multiplication, Rotate left and right.

2 b) Algorithm Flow

To execute and process the data there you have to select the file for storing the data. The process that is carried over is listed in the following steps:

i) Key

1. Key provides the main security layer for processing. To generate the key the time taken for processing will be in milliseconds.
2. The user has to store the key using the generated key that too while storing it must be done using the particular bytes.

INPUT

b byte key preloaded using the c words

array L[0,...,c-1]

Number of rounds r

P_w = odd (e-2)2w)

Q_w = odd (θ-2)2w)

OUTPUT

W bit rounds

Keys S[0,....,2r+3]

ii) Encrypt

1) The key that is generated in the above process is passed for the encryption process. There the function gets initiated.
2) Those functions get started to encrypt the data that is the same as the byte. After that start writing the data that has to be encrypted and store it in the cloud.

INPUT

Plain Text E,F,G, H

Number of rounds = r

Key S[0,....,2r+3]

OUTPUT

Cipher text is E,F,G, H

iii) Decrypt

1. For this process there you have to select the particular files from the cloud and after that start accessing them bypassing the key in the expansion and start generating them.
2. You can start reading out the selected particular file and from there you can start converting them by using the byte arrays.

3. The user has to pass the data along with its key in the decryption format. The outcome will be received in the form of bytes.
4. There start writing the array using the temporary files. Now at this point, the user can start reading from the temporary files.

INPUT

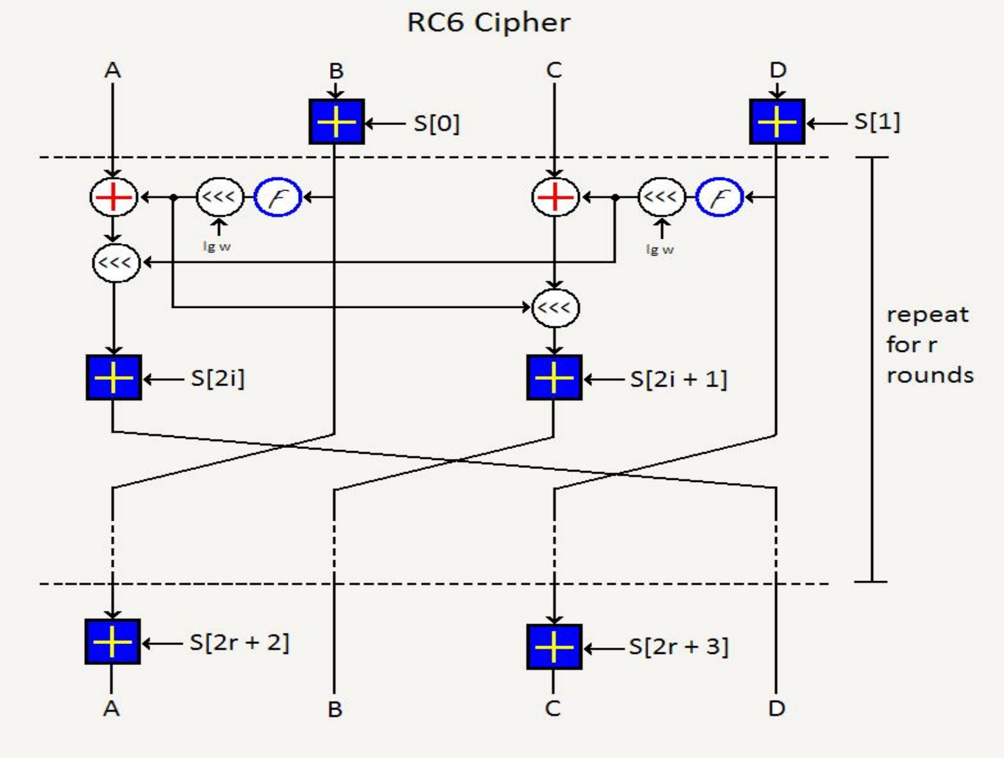
Input registers Plain Text E,F,G, H (Cipher Text)

Number of rounds = r

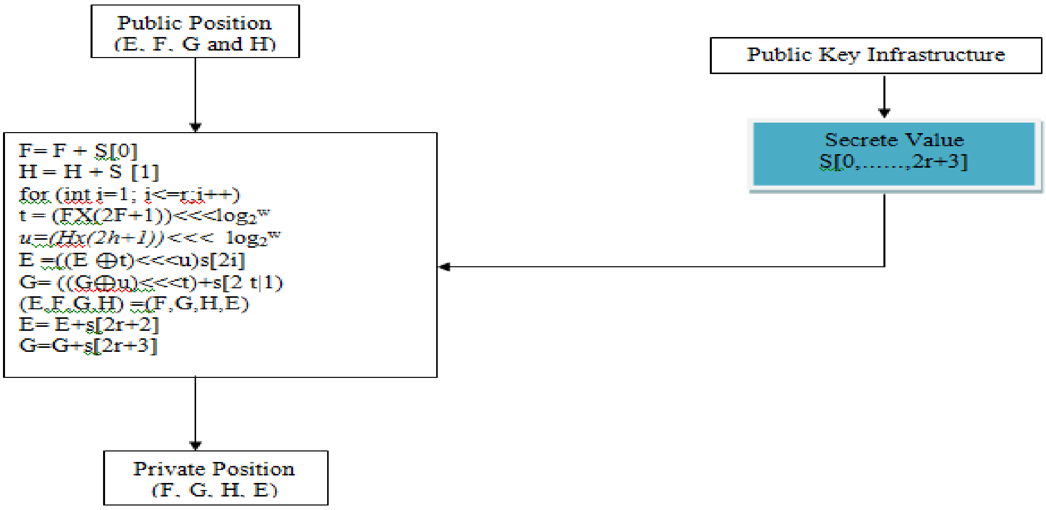
Key S[0,....,2r+3]

OUTPUT

Plain text is E,F,G, H



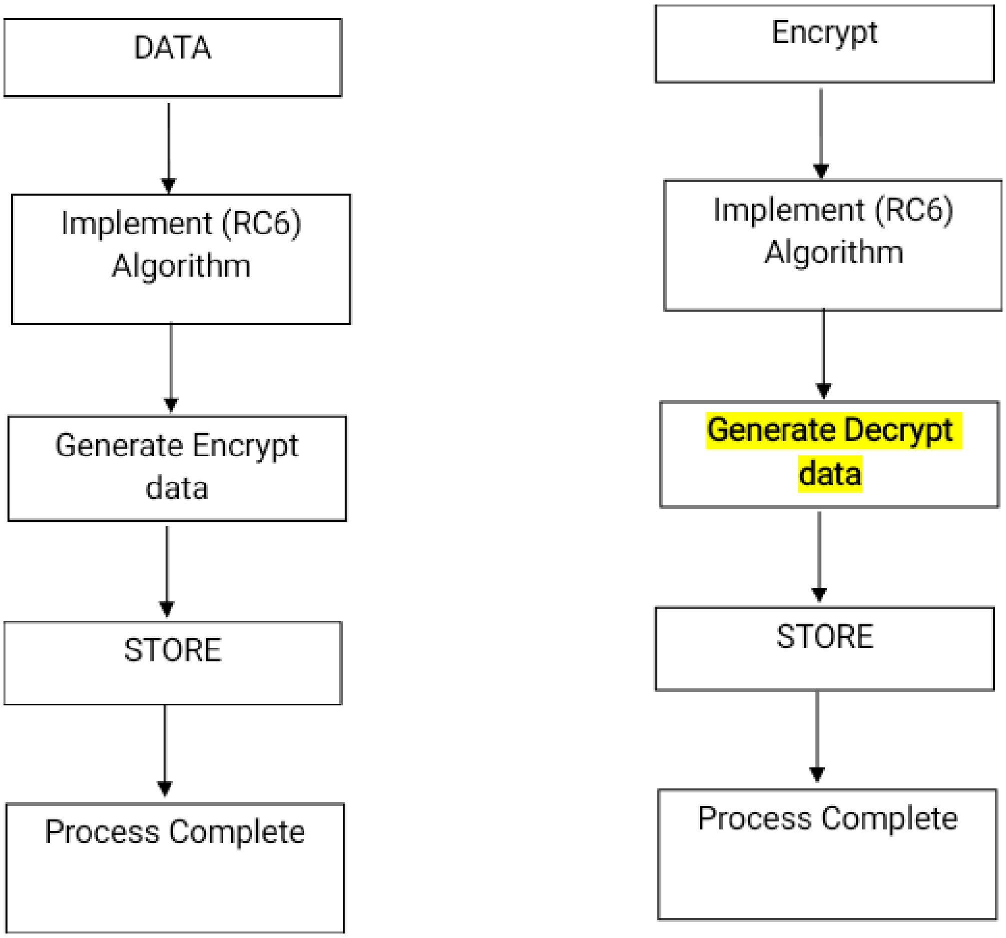
[2]RC6 Algorithm working Process in General[2]



```
F= F + S[0]
H = H + S [1]
for (int i=1; i<=r;i++)
t = (FX(2F+1))<<<$\log_2{}^{w}$
u=(Hx(2h+1))<<< $\log_2{}^{w}$
E =((E ⊕t)<<<u)s[2i]
G= ((G⊕u)<<<t)+s[2 t|1)
(E,F,G,H) =(F,G,H,E)
E= E+s[2r+2]
G=G+s[2r+3]
```

The algorithm flow

Process work flow [ENCRYPTION – DECRYPTION]



3) Experimental analysis

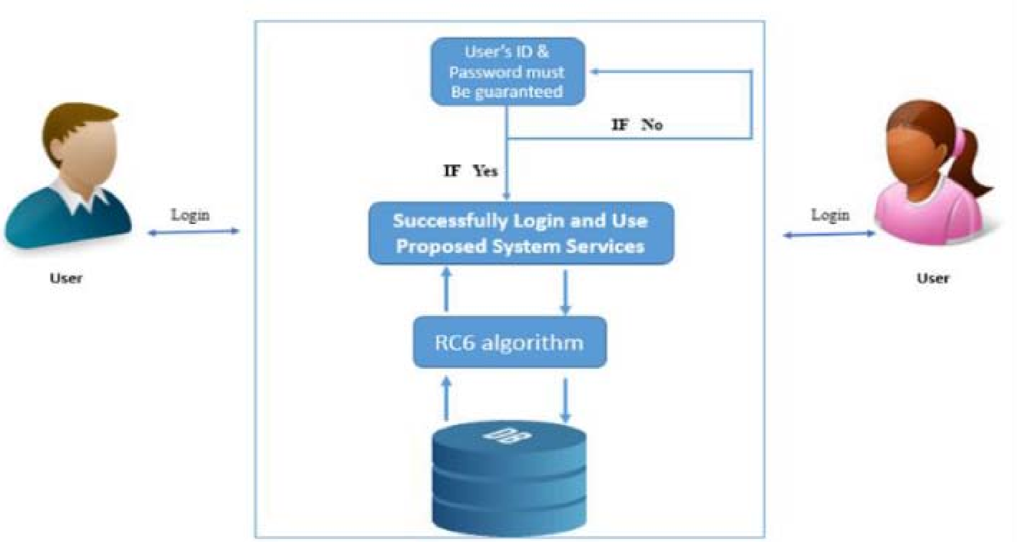
File Size	Time	
	Encrypt	Decrypt
100	14	9
200	20	18
400	36	25
600	67	63

Duration of time taken using RC6 Algorithm

File size = KB

Time = Millisecond

The [4] approximate calculation of time taken is extracted. Based on the size of the file the type that is taken for the encryption and decryption varies.[4] This helps for decreasing the occurrence of the flaw.



[2]Proposed process in Networks [2]

Conclusion

In recent research, the concept of protecting and securing the data was still a little complex task. Even though there are multidimensional algorithm has been implemented. It supports addressing the minute issues that occur. The transactions of the data are done using a secured key. Even there are more proposed works comes into existence simultaneously possibilities of occurrence of error and fault arises. In the forthcoming works, the special algorithm can be built using cloud computing techniques and actively get used in the transaction of data like the RC6 algorithm. That creates the best authentication gateway for the device and the Internet of Things. Also, have an aim for detecting the attacks that are occurred at the cloud servers. While these techniques can be used in the IoT the smarter development, will takes place in the technological world.

Reference

[1] Chanapha Butpheng and Kuo-Hui Yeh: Security and Privacy in IoT cloud Based e – Health systems – A comprehensive Review, Symmetry (2002).

[2] Salim Ali Abbas and Malik Qasim Mohammed: Enhancing Security of Cloud Computing by using RC6 Encryption algorithm, International Journal of Applied Information System, Vol 12 No 8, Ed: Nov 2017, pp 27- 32.

[3] In Lee: Internet of Things (IoT) Cybersecurity: Literature Review and IoT cyber Risk Management, future internet (2020)

[4] Narendra Chandel and Sanjay Mishra: Creation of Secure Cloud Environment using RC6, 2013 International Conference on Intelligent Systems and Signal Processing (ISSP), pp 317-318

[5] Boda Mash :International Law and Cyber crime, Paper presented on the cyber Liability, (2002)

[6] Johm Harauz, M. Kaufman: Data Security in the world of cloud computing, IEEE computer society 2012.

[7] Bi, Z., Xu, L., and Wang, C. (2014), "Internet of Things for Enterprise Systems of Modern Manufacturing," IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, pp. 1537 - 1546 2014

[8] Maha TEBAA, Said EL HAJI: Secure cloud computing through Homorphic Encryption, International Advanced Journal of Advancements in Computing Technology, Vol 5, No 16 (2003)

[9] Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and Other Botnets." computer. vol. 50, no. 7, pp. 80-84, 2017.

[10] Rauter, Tobias, N. Kajtazovic, and C. Kreiner. "Privilege-Based Remote Attestation: Towards Integrity Assurance for Lightweight Clients." ACM Workshop on IoT Privacy, Trust, and Security .ACM, 2015, pp. 3-9.

[11] Zhao, Lu, et al. "ARMor: fully verified software fault isolation." Proceedings of the International Conference on Embedded Software IEEE, 2011:289-298.

[12] Liu, Hui, et al. "Smart Solution, Poor Protection: An Empirical Study of Security and Privacy Issues in Developing and Deploying Smart Home Devices." IoT Security & Privacy Workshop 2017, pp. 13-18.

[13] Conrad, S. K. (1998): Making telehealth a viable component of our national health care system. Prof. Psychol. Res. Pract. 29(6):525–526.

[14] Maryem Neyja, Shahid Mumtaz, Kazi Mohammed Saidul Huq, Sherif Adeshina Busari, Jonathan Rodriguez and Zhenyu Zhou: An IoT-Based E-Health Monitoring System Using ECG Signal. Instituto de Telecomunicações, 3810-193 Aveiro, Portugal, North China Elec- tric Power University.

[15] Davidson, Drew, et al. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution." USENIX Security Symposium. 2013, pp. 463-478.