International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

Securing Health Industry Data using Modern Ceaser Cipher Technique

Sumana Reddy Reddybathula, Kiran Kumar K, Dharsini Vandanapu, Mahitha Guduri

Abstract*: In recent years a wide range of wearable health care applications have been deployed. The rapid increase in wearable devices allows the transfer of patient personal information between different devices, at the same time personal health and wellness information of patients can be attacked. There are many techniques that are used for protecting patient information in medical and wearable devices. In this research a comparative study of the complexity for cyber security architecture and its application in health care industry has been carried out. Using ceaser cipher the encryption and decryption process will be carried out to secure the hospital data from third parties.

Index Terms*: : *Modern ceaser cipher algorithm, securing data, ransom-ware, right-shift, left-shift.

I. INTRODUCTION

Highlight a section as the health care sector continues to offer life-critical services while working to improve treatment and patient care with new technologies, criminals and cyber threat actors look to exploit the vulnerabilities that are coupled with these changes. The following blog series will explore one MS-I SAC analyst's thoughts on today's sources of frustration for health care IT and cybersecurity specialists. The human services industry is tormented by a bunch of cybersecurity-related issues. These issues go from malware that bargains the uprightness of frameworks and security of patients to disseminated forswearing of administration (DDoS) assaults that upset offices' capacity to give tolerant consideration. While other basic framework parts encounter these assaults also, the nature of the human services industry's main goal presents exceptional difficulties. For social insurance, digital assaults can have consequences past monetary misfortune and rupture of protection. Each connection beneath prompts a talk of that extraordinary assault, including genuine precedents of how it showed, the harm and interruption it caused or could have caused if not taken care of legitimately, and proposals on shielding against or alleviating each sort.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author
Sumana Reddy Reddybathula, Student of Koneru Lakshmaiah Education Foundation,
Kiran Kumar K, Professor, Department of ECM, Koneru Lakshmaiah, Education Foundation, Electronics and Computer Science.
Dharsini Vandanapu, Student KL University.
Mahitha Guduri, Student KL University.

- Ransomware
- Data Breaches
- DDoS Attacks
- Insider Threat
- Business Email Compromise and Fraud Scams

This is in no way, shape or form a comprehensive rundown of the sorts of assaults doctor's facilities confront at the same time, rather, a synopsis of a portion of the major and most expensive occurrences influencing doctor's facilities.

RANSOMWARE

Use either SI (MKS) or CGS as primary It is difficult to disregard the ongoing increment in revealing of healing facilities defrauded by ransomware. Ransomware has turned out to be such an issue, to the point that the MS- ISAC, alongside our accomplices at the National Health Information Sharing and Analysis Center (NH-ISAC) and Financial Services Information Sharing and Analysis Center (FS-ISAC), collaborated to have trainings around the nation on the most proficient method to shield against it. Ransomware is a kind of malware that contaminates frameworks and records, rendering them unavailable until the point that a payoff is paid. At the point when this happens in the human services industry, basic procedures are hindered or turned out to be totally inoperable. Doctor's facilities are then compelled to return to using pen and paper, abating the therapeutic procedure and eventually dousing up assets that may somehow or another have been apportioned to the modernization of the doctor's facility.

Ordinarily, ransomware taints unfortunate casualty machines in one of three different ways:

1.through phishing messages containing a pernicious connection
2.by means of a client tapping on a noxious connection
3.by survey and containing malware (malvertising)

Regularly advancing variations and strategies, methods, and techniques (TTPs) make it hard for security specialists to keep up. Moreover, stages, for example, ransomware as a service[i] (RaaS) make it simple for anybody with practically zero specialized expertise to dispatch ransomware assaults against casualties based on their personal preference.

EXAMPLE:

As of late, various healing facilities the nation over were tainted with ransomware by means of obsolete JBoss server programming. In these cases, the assailant transferred malware to the obsolete server with no communication from the person in question, instead of contaminating the healing centers through normal workstations utilized by ordinary staff. Hollywood Presbyterian Hospital in California was one of the doctor's facilities influenced, for a situation which deferred understanding consideration and eventually brought about the clinic paying $17,000 to re-access documents and their system. Performers utilized an open source device, JexBoss, to scan the Internet for powerless JBoss servers, and contaminated systems, paying little mind to what industry they were running on. While there is no complete confirmation, some have hypothesized that the high payoff requests saw in medicinal services related cases demonstrated the digital danger performing artists knew about who they had contaminated. They may have known that gadgets bargained in a contamination procedure are frequently significant to a clinics' central goal, and the ransomware may render them unavailable, deferring understanding consideration while making enormous weight remediate the issue instantly. This weight, joined with the way that healing centers by and large have money related assets available, possibly improves the probability the assailants will be paid.

II. LITERATURE SURVEY

Despite the fact that numerous shields and strategies for electronic health record (EHR) security have been actualized, obstructions to the security and security insurance of EHR frameworks continue. This article introduces the consequences of an orderly writing survey with respect to habitually received security and protection specialized highlights of EHR frameworks. Our incorporation criteria were full articles that managed the security and protection of specialized usage of EHR frameworks distributed in English in friend investigated diaries and gathering procedures somewhere in the range of 1998 and 2013, 55 chose examinations were inspected in detail. We dissected the survey results utilizing two International Organization for Standardization (ISO) standards (29100 and 27002) so as to solidify the examination discoveries[1].

Lately, clinics in Iran - like those in different nations - have encountered developing utilization of computerized health information systems (CHISs), which assume a critical job in the tasks of medical clinics. Be that as it may, the real test of CHIS use is data security. This investigation endeavors to assess CHIS data security hazard the executives at medical clinics of Iran. This connected investigation is an illustrative and cross-sectional research that has been directed in 2015. The information were gathered from 551 emergency clinics of Iran. In view of writing survey, specialists' supposition, and perceptions at five emergency clinics, our concentrated poll was intended to evaluate security hazard the board for CHISs at the concerned medical clinics, which was then sent to all emergency clinics in Iran by the Ministry of Health [2].

Lately a wide scope of wearable IoT social insurance applications have been created and conveyed. The quick increment in wearable gadgets permits the exchange of patient individual data between various gadgets, in the meantime close to home wellbeing and health data of patients can be followed and assaulted. There are numerous procedures that are utilized for ensuring understanding data in medicinal and wearable gadgets. In this exploration a relative investigation of the multifaceted nature for digital security engineering and its application in IoT medicinal services industry has been done. The target of the examination is for shielding social insurance industry from digital assaults concentrating on IoT based human services gadgets. The plan has been actualized on Xilinx Zynq-7000, focusing on XC7Z030-3fbg676 FPGA gadget[3].

III. WORKING PRINCIPLE OF ALGORITHM

ENCRYPTION:

The action of a Caesar cipher is to replace each plaintext letter with a different one a fixed number of places down the alphabet. The cipher illustrated here uses a left shift of three, so that (for example) each occurrence of E in the plaintext becomes B in the cipher text. Here we have used the modern ceaser cipher algorithm and the working principle of this algorithm is of following.

In encryption process there are two levels of encryption. In level 1encryption process replacement of each plaintext letter with different fixed number of places down the alphabet. The cipher illustrated here uses a right shift of certain number (for example: four), so that for each occurrence A in the plaintext becomes E in the cipher text, as well as ‘a’ in the plain text becomes ‘e’ in the cipher text. In level 2 encryption process result of level1 which is in alphabetical order will be again encrypted into numerical order i.e., ASCII values (eg: shift four), so that each occurrence ‘E’ becomes ‘73’ (ASCII value of E is 69 and shift is 4 so that cipher text of level2 becomes 69+4=73). And also ‘h’ becomes ‘108’ (ASCII value of h is 104 and shift is four i.e., 104+4=108) in cipher text.

DECRYPTION:

In modern ceaser cipher technique decryption process is also done in two levels as we have seen encryption is done at two levels. In level1 decryption same number of shift is taken place as in encryption process of level2, so that each occurrence of ‘73’ in the cipher text becomes ‘69’ i.e,(73-number of shifts in level 2 encryption→73-4=69 which is the asci value of E) in level1 decryption. In level2 decryption as the level1 decryption is in ASCII values it places down to alphabets for example ‘69’ in level 1 decryption becomes ‘A’ (69 is the asci value of ‘E’ – shift of level 1 encryption i.e, four→ 69-4=65 which is ASCII value of ‘A’) and we can get the actual encrypted data.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

IV. SECURITY THREATS IN HEALTH INDUSTRY:

Human services applications are exceptionally basic applications and restorative information are exceptionally basic and complex to be secure than other sort of information and applications since it should be very anchored [11]. There are numerous sorts of dangers that may confront the social insurance applications which vary in their causes furthermore, contrast in their answers. A portion of these security dangers are featured in this paper. These security dangers are eavesdropping, impersonation, message modification, and Man-in-the middle.

V. Figures and Tables

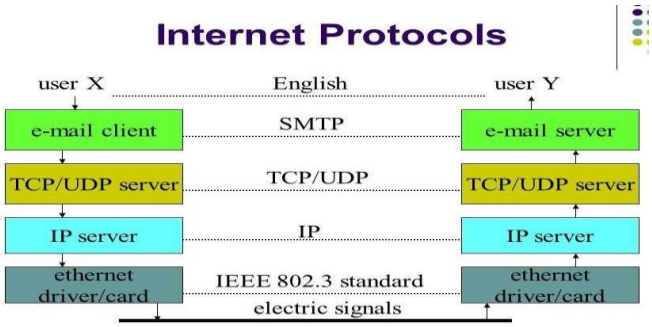


Fig.1 TCP internet protocols

The Transmission Control Convention (TCP) is one of the primary conventions of the Web convention suite. It began in the underlying system execution in which it supplemented the Web Convention (IP).

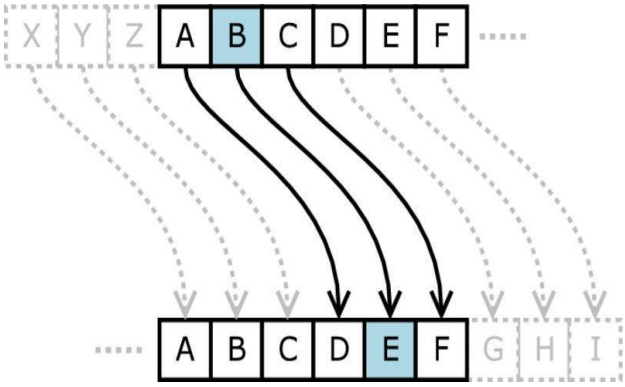


Fig 1.2 encryption level 1

There are 2 levels in encryption process in level1 right shift operation is preformed on the alphabets and for level2 encryption ascii values of those alphabets is taken and right shift operation is again performed on those ascii values.

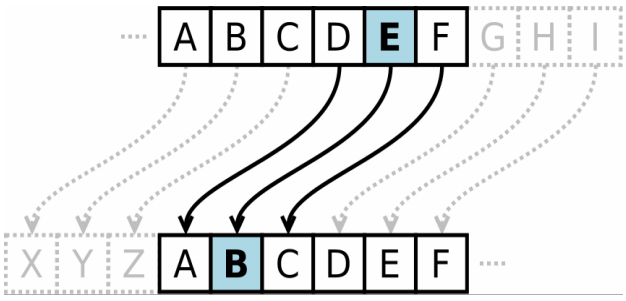


fig1.3 decryption level 2

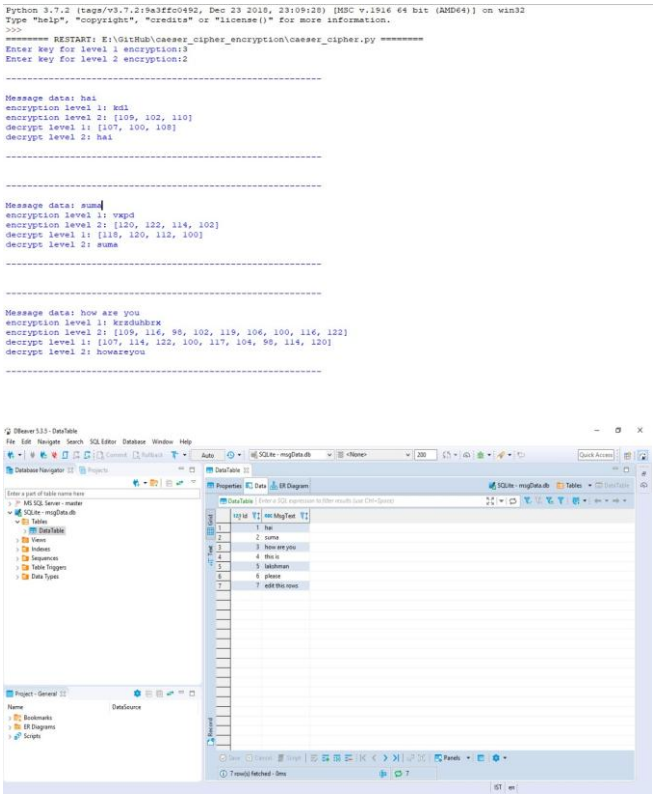
There are also 2 levels in decryption process in level 1decryption process left shift operation is performed on the ascii values and then alphabets of those ascii values are taken and also shift operation is performed on those alphabets in level 2 decryption process.

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
multiply by 3	3	6	9	12	15	18	21	24	27	30	33	36	39
mod 26	3	6	9	12	15	18	21	24	1	4	7	10	13
Cipher text	C	F	I	L	O	R	U	X	A	D	G	J	M

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
multiply by 3	42	45	48	51	54	57	60	63	66	69	72	75	78
mod 26	16	19	22	25	2	5	8	11	14	17	20	23	0
Cipher text	P	S	V	Y	B	E	H	K	M	Q	T	W	Z

fig1.5

VI. EXPECTED RESULTS



These are the results after connecting the database to the python program done in the python shell. By seeing these results we can say that we can secure the hospital data without any threats.

REFERENCES

1. M. Abdalla, J. H. An, M. Bellare, C. Namprempre, "From identification to signatures via the Fiat-Shamir transform: Necessary and sufficient conditions for security and forward-security", *IEEE Trans. Inf. Theory*, vol. IT-54, no. 8, pp. 3631-3646, Aug. 2008.

2. Mohammed Al-Amin, Abdulrahman Olaniyan, "Vigenere Cipher: Trends Review and Possible Modifications", *International Journal of Computer Applications 135*, no. 11, pp. 46-50, Feb 2016.
3. Aditi. Saraswat, Chahat. Khatri, Sudhakar, Prateek. Thakral, Prantik. Biswas, "An Extended Hybridization of Vigenere and Caesar cipher techniques for secure communication", *Elsevier Procedia Computer Science*, vol. 92, pp. 355-360, 2016.
4. G Z. Nacira, A. Abdelaziz, "The θ -Vigenere Cipher Extended to Numerical Data", *Proceedings of International Conference of Information and Communication Technologies: From Theory to Applications*, 2004.
5. J K Pal, J K Mandal, S. Gupta, "Composite Transposition Substitution Chaining Based Cipher Technique", *Proceedings of 16th International Conference on Advanced Computing and Communications*, 2008.
6. I. A. Ismail, M. Amin, H. Diab, "how To Repair the Hill Cipher", *Journal of Zhejiang University Science A*, vol. 7, no. 12, pp. 2022-2030, 2006.
7. Z. Wang, R. B. Lee, "A novel cache architecture with enhanced performance and security", *41st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, 2008.
8. American National Standard Code for Information Interchange X3.4, NY, 1430 Broadway, New York:American National Standards Institute, pp. 10018.
9. H. Feistel, "Cryptography and computer privacy", *Scientific American*, vol. 228, 1973.
10. Prachi Patni, "A Poly-alphabetic Approach to Caesar Cipher Algorithm", *(IJCSIT) International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, pp. 954-959, 2013, ISSN 0975-9646.

VIII. CONCLUSION

This project is aimed to provide security for hospital data by using modern ceaser cipher technique. Encryption and Decryption process are done while sending and receiving the data. The code is developed for this process by using Python IDE. And database connection is also given to the patient's data. Thus we can ensure that we can protect the hospital data by using this technique.

AUTHORS PROFILE

Sumana Reddy Reddybathula Designation: Student College/university: Koneru Lakshmaiah Education Foundation, Stream: Electronics and Computer Science.

Kiran Kumar k, Designation: Professor, Department of ECM, College/university: Koneru Lakshmaiah Education Foundation, Stream: Electronics and Computer Science.

Dharsini Vandanapu, Designation: Student College/university: KL University Stream: Electronics and Computer Science.

Mahitha Guduri, Designation: Student College/university: KL University Stream: Electronics and Computer Science.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication