Chaos Cryptography For Securing Backup File

Ahmad Faisal Abidin, Abdul Aslam Husaini, Nor Surayati Mohamad Usop, Mohamad Afendee Mohamed, Mohd Fadzil Abdul Kadir

Abstract: These days, more people grow dependency on IT infrastructures and relies their decision making on the data stored within a computer system. Data go through some processing to make it useful whereas in other time it is kept within the database. Data availability is a critical issue, the approach is to do backup all the crucial data, and it can be difficult especially a beginner. One of the human errors is easily forgetting things, in this situation a periodic manual backup may be forgotten to do even it's a click away. A hacker looks for the opportunity to attack even as tiny as a day of forgotten backup. This is one of the reason backups must be an automated process. It can be coupled with cryptography as a mean to protect data from theft, alteration, and authenticate. Chaotic cryptography is an application of chaos theory into cryptography, which makes use of a simplex system to produce chaotic value needed for the encryption and decryption. The advantage of chaos cryptography is randomness alike, which creates more complex encryption and decryption key by a concept of confusion and diffusion.

Index Terms: Backup File; Cron Job; Chaotic Cryptography, Confusion and Diffusion, Computer Hacker.

1. INTRODUCTION

CRYPTOGRAPHY is a practice to protect data from theft, alteration, and authenticate. Chaotic cryptography is an application of chaos theory into cryptography. One of the advantages of chaos cryptography is that long-term prediction is impossible. The ergodicity and sensitivity to initial condition also is the important characteristic of secured communications in this cryptography. Finding an alternative to the existing cryptography such as RSA is becoming an interest. Chaotic cryptography is what comes to mind, and day by day more research is done about chaotic cryptography. The key properties of it are the ergodicity, sensitivity on initial conditions and system parameters serve as a scheme to improve security. In addition, it is important to do a daily backup of your files in case of failure to prevent data loss. Failure can be caused by plentiful reasons, including user errors, intruders attack or natural disaster. One of the multiple solutions to keep the availability of file high is the creation of backup. With automated backup user or admin do not need to do it manually every day considering the carelessness of human who sometimes forgets to backup data. To maintain the productiveness and to maintain the trust of the user toward the company as it would be any data that need to be processed in a day.

The fact that hackers may get something from examining the pattern of plaintext or ciphertext and guess the meaning of it can bring a problem to its security of cryptography. Security is another aspect that needs to be examined because there will be chances that a system may be compromised by a hacker. This paper proposes that the backup files should be automatically backed up and encrypted by using chaotic cryptography. Even if the data is unconsciously being stolen without your knowledge, the encrypted data will not be easy to decrypt as it may take many years, and that will be useless.

2 LITERATURE REVIEW

A backup contains a lot of private information about customers which should be protected properly. Mistakes in the backup concept can have a disastrous outcome. The foundations of IT Security and the basics of backups discussed further. For example, encryption reduces availability because the key needs to be available to read the data, yet it raises confidentiality [1]. There are various reasons for making backups for example to mitigate chances of corrupted data. The backup process always needs to be structured carefully. Since backups contain lots of important data in a central location, their security is highly important, so issues of ensuring confidentiality, integrity, and availability are explored in combination with processes that help to determine threat models for actual systems and concepts [2]. A researcher, Duncan Napier suggested in an article [3] about step by step for building a Backup Server using Linux. It suggests the requirement for software, the need for basic network administration utilities such as secure shell, SSH and most interestingly is rsync. Rsync is kind of like copying and synchronizing utility for data remotely or locally present in all of Linux system [4]. It is better and faster than secure copy because rsync can copy only the changes applied, it happens from the same source to the destination the second time. The purpose of monitoring the backup process is making sure the backups are operating well as planned by generating report automatically together with the backup process. The information contained in the report usually is a summary of the backup that happened and the disk space used. Each step of backup can just be completed by using shell scripts function in Linux, and an example of it is included in the article [3]. It is an amazing write-up and useful even for the experienced users of Linux. Tim Cordova stressed on always being prepared for the possibilities of being compromised virtually or physically [5]. The physical aspect of security is emphasized as some compromises are caused by someone having physical access to the system. When the data is out of your watch, always consider the potentials that it will be in someone's hand just a matter of time. Whole disk encryption is a feature that can reduce the risk when using open-source Linux operating system, especially regarding the recent event on stolen government laptop and the data that have been leaked. Next, adding another layer of security by encrypting home directories during initial installation, this step slows down others that try to access data contained in your system while running [5]. Linux OS can utilize an open-source application,

- *Ahmad F Abidin, Faculty of Informatics & Computing, Universiti Sultan Zainal Abidin, Besut Campus, Terengganu, Malaysia*
- *Abdul A Husaini, Faculty of Informatics & Computing, Universiti Sultan Zainal Abidin, Besut Campus, Terengganu, Malaysia*
- *Nor S M Usop, Faculty of Informatics & Computing, Universiti Sultan Zainal Abidin, Besut Campus, Terengganu, Malaysia*
- *Mohamad A Mohamed, Faculty of Informatics & Computing, Universiti Sultan Zainal Abidin, Besut Campus, Terengganu, Malaysia*
- *Mohd F A Kadir, Faculty of Informatics & Computing, Universiti Sultan Zainal Abidin, Besut Campus, Terengganu, Malaysia*

TrueCrypt to create encrypted containers to keep any personal data that you want to keep safe. This grant another layer of security. Two options to choose from, either creating an encrypted file container or creating a volume within a partition/drive. If any of this choice is picked, the volume type as a standard TrueCrypt or hidden TrueCrypt options is given. The interesting things about hidden TrueCrypt options, it creates a container within a container, the volume will mount when the correct password is entered, but in order to mount the hidden container, the password for the hidden volume needs to be inserted. Encryption algorithm and hashes including AES with 256/14 rounds or SHA-512 [6]. SpiderOak is a safe and secure online storage location used for the created encrypted container that is intended for backing up data in the cloud [7]. This company uses two-factor authentication by application of token other than username and password. Your phone will receive the token anytime you log in to the website or device. This two-factor authentication does not ensure safety, but it can make it complex for attackers to take advantage. A SpiderOak application allows you to select your encrypted volume to back up automatically in specific time [7]. This application SpiderOak is a suitable in-home environment where the personal data need to be encrypted on a daily basis [5]. Many applications out there are available, but this is one that is easy to deploy. Warning as it not be an ideal for enterprise company with many agencies. Meanwhile, for the cron job scheduler, it contains of cron daemon which is available in nearly all Linux distributions. It is like a man-ager of scheduled task. When set the specific time to a specific job to run, cron awakes, runs its plan and then sleeps until being called again [8]. Cron is something you use when you want to make something to automatically run more than once. Cron settings can be access to command crontab -e, which then created a crontab file, make the changes there, save it and exit. Each field in the crontab field means something, the time and date to run it with the path or command to run it.

2.1 Cryptography with Chaos

The system is said to be chaotic if it consists of properties such as sensitive to initial condition in that a small changes in the value of a parameter render the output completely the other way around, topo-logically mixing and dense periodic orbit [9]. A study of chaos rooted to the study of non-linear dynamical system, which later was largely used to model real-world phenomenom with chaotic proper-ties with an intention to predict what's coming next. Chaos theory investigates into nonlinear system that are effectively impossible to predict or control such as the turbulence, weather, and stock market. In addition, many physical systems have been identified as chaotic, as well as been designed to be chaotic [10,11,12,13,14]. On the other hand, the behavior of chaotic has been recognized as useful for and interchangeably with cryptography [15]. Cryptography is important to disguise a normal message to the message which cannot be read by unauthorised person. Chaos was made possible for cryptography and has been greatly studied for cryptography technique. Chaos based Baptista [15] proposed to us that it is possible to encrypt a message using the simple low-dimensional and chaotic logistic equation. Encrypt each character of the message as the integer number of iterations performed in the logistic equation, to transfer the trajectory from an initial condition towards an E-interval inside the chaotic logistic attractor Chaos was first applied for transmitting signal as proposed by Pecora and Carroll, [16] they showed it by synchronized trajectories of two chaotic circuit and the chaotic signal produced to conceal the message. Using chaos for sending messages and it can be con-trolled by using small changes. The message is then recovered by the receiver, which assumes that some alphabets are associated with the time of arrival [15]. New cryptographic techniques are based on number theory or algebra concept. Chaos is another branch out from the nonlinear dynamics and has been widely researched [17]. Nonlinear system exhibits chaotic behavior which looks random. This origin of randomness is totally a result of the deterministic process. The main characteristic of chaos is its tremendous sensitivity to the initial condition of the system. Pecora and Carroll in the early 1990's [16] discovered that chaos theory possibly can help in securing communication. Its major properties are sensitive to the initial condition, ergodicity and sys-tem parameters are key factors in building secure communications based on chaos. In recent years, it is stated that chaotic system can be an alternative to the currently existing system as RSA, ECC, and others [18,19,20]. Both hardware and software made up of chaotic systems are now available which can work on encrypting decrypting and data. From the three characteristics of chaos namely the sensitivity of initial condition, ergodicity, and mixing [18], sensitive towards the initial condition means that in an initial state of the non-linear system, the next state of the system can be known. Yet it becomes chaotic when running in long-term which makes it hard for prediction. The two different trajectories which are very close at the beginning become split and spread after sometimes. Ergodicity is the characteristic when a trajectory is close to its previous state, even its wandering to next state is important to apply cryptography. Spread of value even in small changes of initial condition in a chaotic system in which the mixing property shows.

3 METHODOLOGY

The language C++ is used to write the code of encryption and decryption of this chaotic cryptography. There is no user interface for this as it supposed to be an automated process. The source and destination files are already specified in the C++ code even before compiling. For the encryption scheme, the algorithm involve is the logistic equation (1).

$$x = r \cdot x \cdot (1 - x) \qquad (1)$$

where r is parameter or coefficient; x is the initial value; these two values are needed to run the equation.

As other cryptography, this chaotic cryptography involves two keys that only the admin known that is a parameter, r, and initial value, x. The value of r we usually set between 3.5 and 4, because only these values displays chaotic behavior of the number of x produced when inserted. While for the initial value x, as long as x value is between 0 and 1, not more than 1 and less than 0, it will be accepted. When the value of x is more than 1 and less than 0, the result of the number of x is a negative number. The equation will keep running to calculate until the encryption finished. The new value of x produced will find to match that which fit the minimum and maximum value set for each character. The equation will repeat until it finds the suitable value.

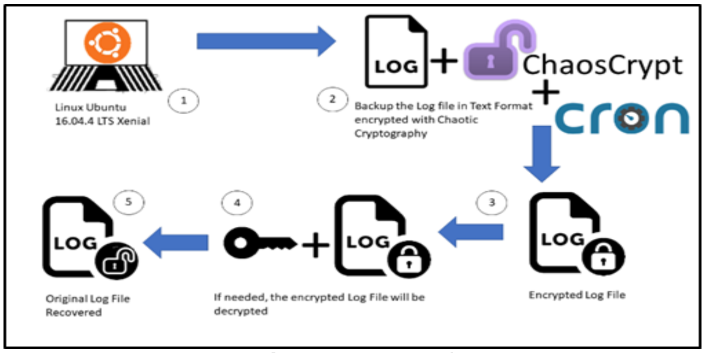

Linux Ubuntu
16.04.4 LTS Xenial
1
LOG
ChaosCrypt
cron
2
Backup the Log file in Text Format encrypted with Chaotic Cryptography
3
LOG
Encrypted Log File
4
LOG
If needed, the encrypted Log File will be decrypted
5
LOG
Original Log File Recovered

***Fig. 1**. Framework*

3.1 Framework

Framework can help to guide and configure out what tools and practices essential to complete a project. Refer to Fig. 1, for number label in it with explanations below.

a) This project was deployed in a Linux environment, Linux Ubuntu 16.04.4 LTS Xenial using Virtual Machine with VMware Workstation 14 Player.
b) Important Log file is chosen in its source directory to back up by cron regularly with Chaotic Cryptography of its content.
c) The Log file is encrypted with chaotic cryptography which the content now will be in number form.
d) If the Log file needs to recover by user or admin, then decryption program will then run on the encrypted log file.
e) After undergoing decryption, the Log file now can be read again in original text form.

3.2 Encryption Scheme

For this section, the encryption procedure will first be translated into pseudocode. The pseudocode is a simple sequence of steps of code to solve problems. It will be too long of code to show how all the character is encrypted, so only example on the character ‘a’ is shown at the pseudocode in Fig. 2.

```
Start
xval = 0.02 // Initial value of x to be insert into equation
r = 3.78 // Another coefficient value in the equation
i = 1 // To calculate iteration value, cycle number equation repeated
while (true) {
xval=r*xval*(1-xval) // Our main equation run to calculate new value of x
char_a = xval // char_a represent character ‘a’
if (char_a>0.6875022 and char_a<0.6979189) {
break
// If the new value x fits between maximum number and minimum number set, then break
}
i = i+1
}
Output char_a // Encrypted character
End
```

***Fig. 2**. Encryption Pseudocode*

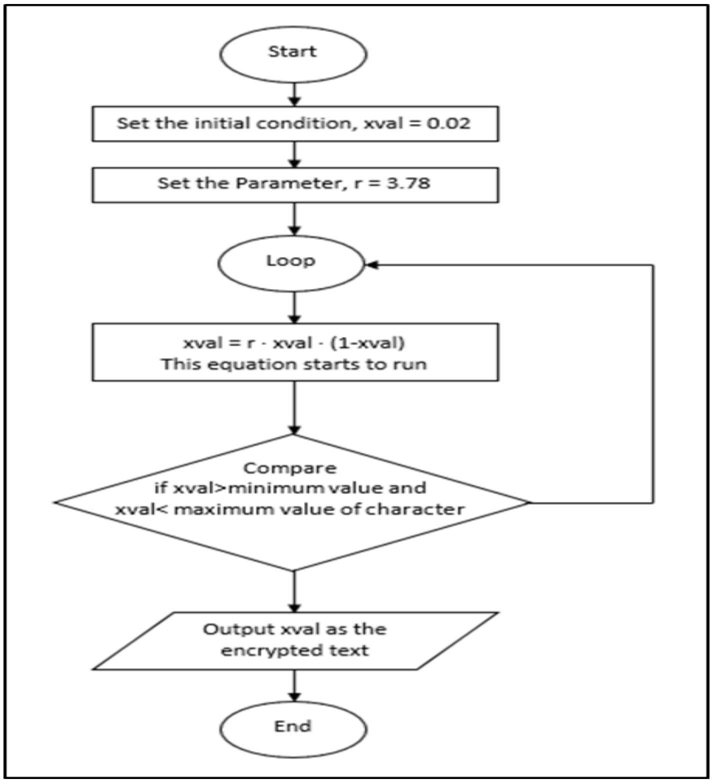

Start
Set the initial condition, xval = 0.02
Set the Parameter, r = 3.78
Loop
xval = r · xval · (1-xval)
This equation starts to run
Compare
if xval>minimum value and
xval< maximum value of character
Output xval as the encrypted text
End

***Fig. 3**. Encryption Flowchart*

3.2.1 Encryption Flowchart

The Fig. 3 explains how the algorithm of the encryption works on the input text. Admin will set the initial condition and parameter of the logistic equation which acts as a key in this cryptography. Then, the equation will run and find the value that suits each character. The value that suits each character is according to the minimum value and maximum value that we already set to each character. If the value output by the equation suits this, then the value becomes the encrypted character.

3.3 Decryption Scheme

The respective decryption pseudocode is shown in Fig. 4.

```
Start
read file_ // Read the content of a file
if (char_a>0.6875022 and char_a<0.6979189) {
//compare the content(number) to which character
Output “a” // substitute a to number if true
}
End
```

***Fig. 4**. Decryption Pseudocode*

The example in Fig. 4 shows how the character ‘a’ is decrypted. The character ‘a’ is located between value 0.6875022 and 0.6979189.

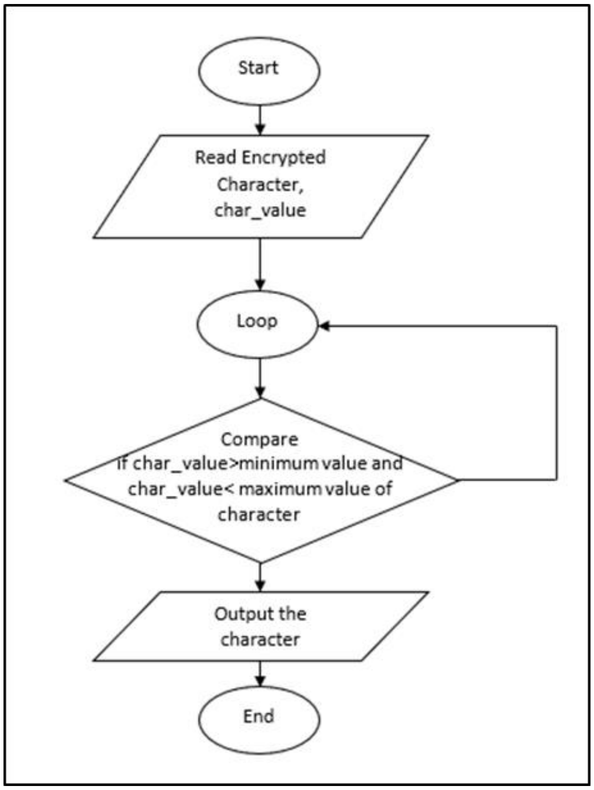

Start
Read Encrypted Character, char_value
Loop
Compare if char_value>minimum value and char_value< maximum value of character
Output the character
End

***Fig. 5**. Decryption Flowchart*

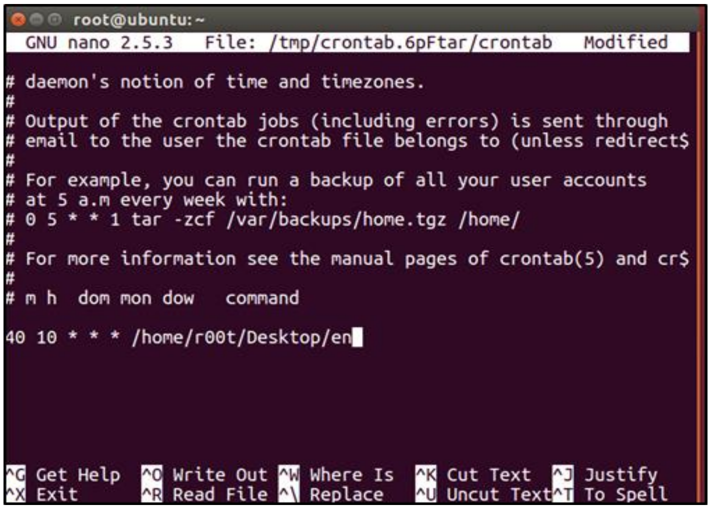
3.3.1 Decryption Flowchart

Based on Fig. 5, the content of the file will be read value by value; then it compares to find the match of which character, if found the character will be output to substitute the encrypted value just now.

4 IMPLEMENTATION

4.1 Automated Process

Crontab in Linux is useful for running task occasionally on a prearranged schedule. Any user can store their crontab files and usually in the directory /etc. or a subdirectory of /etc. in Linux which only system admin can change. Crontab in this project will be responsible for creating a backup of a file daily along with the chaotic cryptography. The crontab syntax includes six fields; the fields are where to define the date and time then followed by a shell command to be executed.



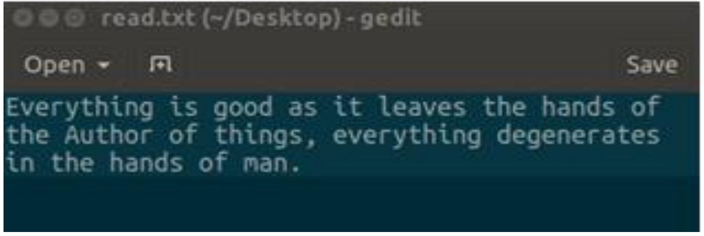
```
  GNU nano 2.5.3    File: /tmp/crontab.6pFtar/crontab    Modified

# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirect$
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cr$
#
# m h  dom mon dow   command

40 10 * * * /home/r00t/Desktop/en




^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell
```

***Fig. 6**. Initializing of Encryption process*

According to Fig. 6, the process is set to run encryption program in 10.40 a.m. every day. The name of the encryption program is ‘en’.

4.2 Results

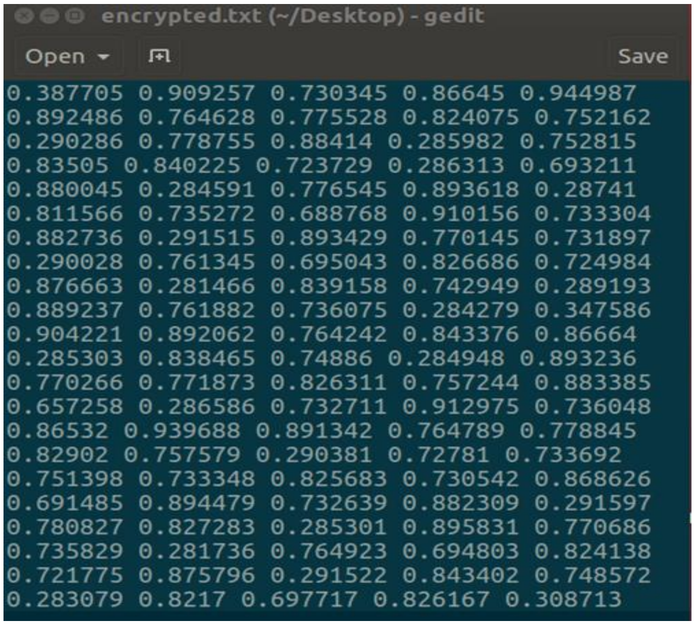
The C++ Program that we encoded will then run on a daily basis and encrypt the text file is that already set.



```
Everything is good as it leaves the hands of
the Author of things, everything degenerates
in the hands of man.
```

***Fig. 7**. Sample Input Text*

Fig. 7 is the text file where it will be then encrypted using chaotic cryptography as we proposed. The result of this encryption is shown in Fig. 8.



```
0.387705 0.909257 0.730345 0.86645 0.944987
0.892486 0.764628 0.775528 0.824075 0.752162
0.290286 0.778755 0.88414 0.285982 0.752815
0.83505 0.840225 0.723729 0.286313 0.693211
0.880045 0.284591 0.776545 0.893618 0.28741
0.811566 0.735272 0.688768 0.910156 0.733304
0.882736 0.291515 0.893429 0.770145 0.731897
0.290028 0.761345 0.695043 0.826686 0.724984
0.876663 0.281466 0.839158 0.742949 0.289193
0.889237 0.761882 0.736075 0.284279 0.347586
0.904221 0.892062 0.764242 0.843376 0.86664
0.285303 0.838465 0.74886 0.284948 0.893236
0.770266 0.771873 0.826311 0.757244 0.883385
0.657258 0.286586 0.732711 0.912975 0.736048
0.86532 0.939688 0.891342 0.764789 0.778845
0.82902 0.757579 0.290381 0.72781 0.733692
0.751398 0.733348 0.825683 0.730542 0.868626
0.691485 0.894479 0.732639 0.882309 0.291597
0.780827 0.827283 0.285301 0.895831 0.770686
0.735829 0.281736 0.764923 0.694803 0.824138
0.721775 0.875796 0.291522 0.843402 0.748572
0.283079 0.8217 0.697717 0.826167 0.308713
```

***Fig. 8**. Encrypted Input Text*

The program will then encrypt each character into six decimal places of number. From the result, we can see that even though it is the same character in which is ‘g,’ the encrypted character ‘g’ is 0.752162 (10th value) and 0.752815(15th value) respectively. This is some quality in cryptography that we want which creates confusion-diffusion to the person who tries to crack this.

5 CONCLUSION

Availability of data is about the data that can be accessed anytime by an authorized person when needed. The data is only valuable if it can be accessed when required, Distributed Denial of Service, stealing of data is common attack toward network devices. Backup of a file is a layer of security to protect data from loss and maintain high availability. Periodically doing file backup can limit the risk of dam-age and restore services of data on standby in case anything hap-pens. Moreover, cryptography is a study to protect data from being com-promised by using written certain code that allows it to be kept secret. Combine chaotic cryptography with backup process making it more secure as it adds another layer of security with the data. The application of cryptography is commonly used in information technology; it can be seen anywhere including website, transmitting message or signal, store data, etcetera. This paper was focused on the study of chaotic cryptography with backup of important files to improve its security if compromised. New theoretical properties of chaotic system are being developed more and with more security features to improve in mind. In this work only uses logistic equation as the main algorithm and with the concept of chaotic cryptography and its characteristic to apply. This project is just a small piece of big idea of chaotic cryptography, which does not even touch about Baptista method, Lorenz attractor, Baker map, Cubic map, Henon map, and others new invention to enhance the weakness of old chaotic cryptography.

ACKNOWLEDGMENT

This project is partially funded by the Research Management, Innovation & Commercialization Center, Universiti Sultan Zainal Abidin.

REFERENCES

[1] Pritz, Florian. “Concept of a Server Based Open Source Backup Process with an Emphasis on IT Security”. Diss. Technische Universität Wien, 2016.
[2] Hasan, Ragib, et al. "Toward a threat model for storage systems." Proceedings of the 2005 ACM workshop on Storage security and survivability. ACM, 2005.
[3] Napier, Duncan. "Build a Home Terabyte Backup System Using Linux." Linux Journal, 2006.
[4] Filgueira, Rosa, et al. "FAST: flexible automated synchronization transfer." Proceedings of the sixth international workshop on Data intensive distributed computing. ACM, 2014.
[5] Cordova, Tim. "Encrypted backup solution: Home Paranoia Edition." Linux Journal, 2014.
[6] Brož, Milan, and Václav Matyáš. "The TrueCrypt on-disk format-an independent view." IEEE Secur Priv 12(3), 74-77, 2014.
[7] Mohtasebi, SeyedHossein, Ali Dehghantanha, and K-KR Choo. "Cloud storage forensics: analysis of data remnants on SpiderOak, JustCloud, and pCloud." Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, 205-246, 2017.
[8] Keller, Michael S. "Take command: cron: Job scheduler." Linux Journal, 1999.
[9] Liu Y., Chen L. “A Survey of Chaos Theory.” In: Chaos in Attitude Dynamics of Spacecraft. Springer, Berlin, Heidelberg, 2013.
[10] K. E. Chlouverakis and J. C. Sprott. “Chaotic Hyperjerk Systems.” Chaos, Solitons & Fractals 28, 739–746. 2005.
[11] Sambas, A., Mamat, M., Vaidyanathan, S, Mohamed, M.A., Mada Sanjaya, W.S. “A new 4-D chaotic system with hidden attractor and its circuit implementation.” International Journal of Engineering and Technology(UAE) 7(3):1245-1250, 2018.
[12] Pehlivan, I., Uyaroglu, Y. “A new chaotic attractor from general Lorenz system family and its electronic experimental implementation.” Turk J Elec Eng & Comp Sci 18(2): 171-184, 2010.
[13] Vaidyanathan, S., Sambas, A., Mohamed, M.A., Mamat, M., Mada Sanjaya, W.S. “A new hyperchaotic hyperjerk system with three nonlinear terms, its synchronization and circuit simulation.” International Journal of Engineering and Technology(UAE) 7(3): 1585-1592, 2018.
[14] Sambas, A., Mamat, M., Vaidyanathan, S., Mohamed, M.A., Mada Sanjaya, W.S., Mujiarto. “A novel chaotic hidden attractor, its synchronization and circuit implementation.” WSEAS Transactions on Systems and Control 13, 345-352, 2018.
[15] Baptista, M. S. "Cryptography with chaos." Physics letters A 240.1-2 50-54, 1998.
[16] Pecora, Louis M., Carroll, T. L., “Synchronization in chaotic systems.” Phys. Rev. Lett. 64, 821-825, 1990.
[17] Lawande, Q. V., B. R. Ivan, and S. D. Dhodapkar. "Chaos based cryptography: a new approach to secure communications." BARC newsletter 258, 2005.
[18] Guttman, Barbara, Edward A. Roback. An introduction to computer security: the NIST handbook. DIANE Publishing, 1995.

[19] Buchmann, J, May, A., Vollmer, U. "Perspectives for cryptographic long-term security." Communications of the ACM 49(9), 50-55, 2006.
[20] Mohamed, M.A. “A survey on elliptic curve cryptography.” Applied Mathematical Sciences, 8(153-156), 7665-7691, 2014.