TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 6601 - 6604

A Two Factor Key Authentication for End to End Decryption

T. Vijay kumar[1], Dr. Sybicynthia. G[2]

[1]UG Scholar, Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences
[2]Professor, Department of CSE, Saveetha School of Engineering, SIMATS
vijaytulluri8@gmail.com[1], cynthia.sybi@gmail.com[2]

Article Info
Volume 82
Page Number: 6601 - 6604
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 01 February 2020*

Abstract
The accessing of the other data from their system is occurring as common. By using their system as the main server and fetching the parol of another system. To reduce these kinds of activities the two way system has been implemented in this paper. The person who can access the other devices or fetching the data they need to first enter the pin. The pin can be change randomly so the opponent can struggle to fetches the data and the other factor is the data are in the encrypted pattern. So when they get to fetches the data the original content of the data cannot be available in the server. The two factors provide a high data security to the system and the cloud communication.

Keywords: *Authentication, struggle, encrypted pattern*

1. Introduction

In the recent survey most of the people using digital technology. They are living in the digital world. The personal dossier of each individual they gets upload into the social website and in the Google accounts. The dossier which is get upload can be gets easily accessed by the third party affiliate. Nebula enumerate is the main technique which act as the pillar for this digital process. The nebula enumerate can be done only in the presence of the internet. Dossier that can be searched by the individual is stored in the nebula it act as extended scaffold with huge anamnesis space. This technique can be demonstrate by the example in the online there are various application are available each have the unique requirements and needs when we download and enter into the applications they can ask several personal dossier and the acceptance of the terms and the condition if we want to use this app we need to performs this conditions. Dossier emporium in the nebula can be differentiating into private groove, public groove and the intermediate groove. The private groove that contains the dossier of the each individual person in a separate location groove of the nebula. The public groove which contains the details of the affiliates in the web groove that can be easily accessed by anyone.

The third groove is the intermediate groove in which it can be used in the corporate and in the industries. To make this dossier set to safe the bilateral key factor is used which makes the use of the personal content of the individual from the pirated person. To make it secure the various contrivances has been involved but this contrivance when compared to one something else there is some drawbacks which leads there is some back end of opening to access the dossier set. To make it more secured a specialized method has been takes place which is the AES. This contrivance is tested in various which is act as barrier to prevent the dossier collecting from the pirated persons. Hacker's feels difficult to fetching the dossier from the set because of using the contrivance which is much protective and use of bilateral key factor which is provides a linear groove.

Each online section has the particular website in which the major content has been declared in the public mode which is much visible to the customers about the industries. The design of the web can be took place in two parts of the section one is the front end and the back end. The front end is the people visiting the web design and can bale to interface with the website. The back end is the coding part section they design and in which basis the web could be operate. The dossier in the nebula can be takes place from any location from any part of the world

January - February 2020
ISSN: 0193 - 4120 Page No. 6601 - 6604

without the loss of single set of dossier. To full fill the customers' satisfaction and free from fear of thefting the personal dossier this nebula scaffold act as safe guard from preventing the use of the set inpatternion. Set which is get upload can be gets easily accessed by the third party affiliate. Nebula enumerate is the main technique which act as the pillar for this digital process. The nebula enumerate can be done only in the presence of the internet. The emporium capacity of the dossier can be in vast extent, fetching of dossier is not easy. For each dossier the parol is provided to make the dossier more confidential and secured. The common division of these three grooves is more safe by using the bilateral key factor and the AES contrivance, Here the dossier are in encrypted form preventing fetching from the pirated person.

2. Literature Survey

B. Waters et., al., proposed users can be increases day by day and the vast numbers of nebula position gets occupied by the users. Due to the increase of the users the dossier accumulation can be much high so the issues of collateral maintenance are arises. To make the inpatternion much confidential, secured. So the increase in the technology hackers fetches the inpatternion in some sort of theft method. To avoid this some research has been took place and then they finally gets a solution to avoid the fetching of dossier by the pirated person. The private latchkey has been generated for the each contaminated dossier set. The dossier can be secured within the latchkey. In this paper they proposed the use of the secured latchkey which is the differential man wave latchkey which is combined with the AES. This latchkey is more secured even when the technical or the hackers team try to break the latchkey, the dossier is get surrounded by the latchkey of fire wall. So the fetching of the dossier is difficult. When they find the latchkey there is the something else inner latchkey which can be changing every period of time. So the dossier fetching is not possible in this method. The dossier collateral is get differentiate into three different categories which can be separated depends upon the efficient of collateral maintained. The vast emporium area can be properly maintained by applying the contrivance in the nebula scaffold for the effective and proper maintains of dossier [1].

S. S. Chaw the et., al., proposed the worlds technology gets developed dossier sharing took place in the nebula via the dossier transfer medium. The dossier can be allocated in the segments of partition in the nebula. Each and every dossier can be arranged in the proper space with the named groove. The groove can be designed with the efficient amount of dossier emporium. As the technology increases at the same time there are some drawbacks is too get increases is the hacking of the personal dossier of the individual in the dossier emporium groove. The hacking can be took place because of the lack of the collateral emporium of the inpatternion. The popularity and the use of the nebula increases the collateral is get decreased due to the maintenance. At the time of dossier sharing the inpatternion can be hacked. From the web retainer by finding the ip address of the particular retainer and the dossier can be easily hacked. In this paper they manly says about the inpatternion collateral in the set that can be act as barrier to the third party who can accessing the dossier in the required and the sufficient anamnesis [2].

M. Massoth et., al., proposed Most of the business people are using the nebula type of dossier sharing from on to something else. They did not care about the location and the emporium and the long distance communication. When the dossier is get transferred from the retainer to retainer communication by knowing the retainer IP address the others affiliates can easily fetches the dossier. The dossier which is much confidential but it gets shared by the other affiliates. This situation is get arises due to the lack of the collateral maintenance in the system architecture. The system can be monitored by the web developing affiliates at the time of transferring the dossier the signal is generated in the serial monitor that shows the some dossier is get transfer from one node to the something else node . In this paper they proposed about the collateral maintenance of the dossier sharing through the internet. The hash code is provided which is act as collateral guard for the dossier sharing in which the dossier can be secured in the both transfer and the receiver end. The both node affiliates have to log on to the hash code so that the files get opened [3].

M. Alzomai., al., proposed the about the collateral issues in the dossier emporium nebula. This paper also presents the dossier gets easily fetches by the some of the people who needs the dossier from the particular party. The dossier can be directly sent through the retainer without changing in any pattern and the minimum of collateral in the dossier allocation groove and in the sharing precinct. This dossier theft can be reduced by the providing the dossier in the encrypted and decrypted form. So the dossier which is get transferred from the sender affiliate the dossier is encrypted and the content of the dossier is not able to read by the human it is machine pattern so the hackers who fetched the dossier from the retainer they can't able to get the content in the file it is of useless file when the dossier gets received by the receiver node they can bale to decrypted the file then the original content of the file gets retrieved. By using this method the dossier becomes much secured and efficient and it is in collaborated with the AES contrivance [4].

P. Tanvi., al., proposed today's world facing the collateral issues in the digital environment. Before some years if we need to theft the dossier from the one person they directly go to them and secretly stoles the dossier file. But now as technology gets improved the dossier gathering is much easy they can fetches from the one place with the some back end code. The code can be created in the web retainer and it particularly maintains the retainer the sharing of the dossier between the two nodes. This collateral lack is gets avoided by the use of the use of the incorruption. The incorruption can be

January - February 2020
ISSN: 0193 - 4120 Page No. **6601 - 6604**

undergoes into some several types which is the 64 bit it can allocate the anamnesis size same as of that and the 128 bit of anamnesis it gets allocated same to that and the 256 bit anamnesis. Based upon this size the dossier can be encrypted to the particular anamnesis sort [5].

D. van Thanh et., al., proposed the unique contrivance to maintain the collateral in the online dossier transfer. Here it uses the two mainly based contrivances which can maintain the dossier in confidential manner. The dossier is encrypted in the sender node groove. The incorruption of the dossier can be involved in two different steps one is the proper upload of the dossier in the nebula and the other one is the proper download of the dossier file from the nebula. The proper which denotes the avoid the missing of the setup files and the packages in the files sets. The dossier which is gets encrypted to particular anamnesis size before uploading into the nebula and the dossier is get decrypted after downloading from the nebula. The dossier transferring gets safe between the two medium grooves. During the incorruption and elucidation the specific tool latchkey has been provided. After done both the process we want to login to the latchkey it act as the parol for the secured dossier section [6].

T. Moors., al., proposed nebula sharing is not only involved the dossier files transfer in also involves the sharing of the money from the one account to the something else account. To make it much secured in this money transferring here much and more corporate are involved in sharing of the money through the online payment. The payment can be done in the retainer. To avoid the theft of the dossier and the money involves a scheme of ATP accessing of third party it makes secured from the dossier accessing by an unknown affiliates. In this paper they proposed involve of the AES contrivance and the hash code detection. They can be done along with the dossier transfer where the incorruption has been made and the receiver groove the dossier gets decrypted after that the verification code has been sent to the required section. After that applying latchkey they can be easily logged on to the file. After that file can be easily gets read by the users and gets safe of fetching the dossier [7].

J. Stook., al., proposed current situation the companies who having the own nebulas are Google, IBM etc., They are the major distributing of nebula emporium to the many clients in the world wide. The dossier can be segregated by using the dossier mining technology in which the separation of the dossier can be done in the nebula. On the time of this process the dossier can be hacked by the third party due to the lack of collateral management in the system. The collateral can be increased by the use of the technique AES contrivance. Dossier file from the nebula. The proper which denotes avoid the missing of the setup files and the packages in the files sets. The dossier which is gets encrypted to particular anamnesis size before uploading into the nebula and the dossier is get decrypted after downloading from the nebula. The dossier transferring gets safe between the two medium grooves. This contrivance can be used to safeguard the dossier files from the unknown party. They generate a latchkey when the affiliate uploads the details in the public precinct. When the other can wants to view the details they needed to login with the latchkey which is being used by the other affiliates [8].

A. Mpitziopoulos et., al., proposed the nebula enumerate is the emporium of the dossier set of the one users with the large amount of anamnesis allocation. They anamnesis can be provided to each affiliates as in the range of the giga bytes. The anamnesis bytes can be declared in technical terms. The users wants to upload the dossier in the nebula set after uploading the dossier the contact between the dossier and the individual affiliate who upload the code is cleared. On the upcoming times the process can be took by the nebula services. So there is some lack of collateral in the dossier management system. The collateral can be increased by the use of the ATP which is the accessing of the third party and the AES and the hash code segment. In which the dossier can be provided by the customers are accessed by them and the receiver so there is no theft in the dossier. Verification has been made in the particular time of elucidation. By using this dossier theft is reduced and the inpatternion are in the safe position. This system has been first implemented by the Amazon web service in dealing the windows technology [9].

Nagasai Lohitha et., al., proposed about the collateral of the dossier in the nebula management system. In the current hacking world it is difficult to safe guard once private inpatternion. The hacking has been done from the one retainer to something else retainer through the latchkey of the main retainer. To protect the inpatternion in this paper they proposes AES and the effective cyber detecting contrivance to prevent the dossier theft from the something else retainer and the special technique is that it can clearly shows that retainer id and their location from where the dossier is being fetched. This collateral system can generates a latchkey to unlock the file. The latchkey can be changed periodically at every instances of time so that the dossier hacking is difficult. The several nebula scaffolds offers these features to the corporate companies. In future this system has been implemented in all over the world [10].

3. Review In Data Collateral In Cloud Enumerate Using Ames Under Heroku Cloud

This paper mainly says about the accessing of the data and the system without their response. These can be reduced by the two way factor in the system the factor which mainly shows the parol and the cipher of the data. The unknown person who wants to access the data and the system they first need to verify the parol. As that the parol can be varied according to that. The second factor is the decryption. The data are in the encrypted form we want to decrypt it.

References

January - February 2020
ISSN: 0193 - 4120 Page No. **6601 - 6604**

[1] B. Waters, "Ciphertext-policy attribute-based cipher: an expressive, efficient, and provably secure realization," in Proceedings of the 14th international conference on Practice and theory in public key cryptography conference on Public key cryptography, Berlin, Heidelberg, 2011, pp. 53-70.

[2] S. S. Chaw the, "Beacon Placement for Indoor Localization using Bluetooth," in Intelligent Transportation Systems, 2008. ITSC 2008. 11th International IEEE Conference on, 2008, pp. 980-985.

[3] M. Massoth and T. Bingel, "Performance of Different Mobile Payment Service Concepts Compared with a NFC-Based Solution," in Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on, 2009, pp. 205-210.

[4] M. Alzomai and A. Jøsang, "The Mobile Phone as a Multi OTP Device Using Trusted Computing," in Network and System Security (NSS), 2010 4th International Conference on, 2010, pp. 75-82.

[5] P. Tanvi, G. Sonal, and S. M. Kumar, "Token Based Authentication Using Mobile Phone," in Communication Systems and Network Technologies (CSNT), 2011 International Conference on, 2011, pp. 85-88.

[6] D. van Thanh, I. Jrstad, T. Jonvik, and D. van Thuan, "Strong authentication with mobile phone as security token," in Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on, 2009, pp. 777-782.

[7] T. Moors, M. Mei, and A. Salim, "Using short-range communication to control mobile device functionality," Personal and Ubiquitous Computing, vol. 12, pp. 11-18, 2008.

[8] J. Stook, "Planning an indoor navigation service for a smartphone with WiFi fingerprinting localization," Delft University of Technology, 2011.

[9] J. Bettencourt, A. Sahai, and B. Waters, "Ciphertext-Policy AttributeBased Cipher," in Security and Privacy, 2007. SP '07. IEEE Symposium on, 2007, pp. 321-334.

[10] S.V. Manikanthan, T.Padmapriya, “A Secured Multi-Level Key Management Technique for Intensified Wireless Sensor Network”, International Journal of Recent Technology and Engineering, Vol. 7, issue6s2, 2019. https://www.ijrte.org/wp-content/uploads/papers/v7i6s2/F10720476S219.pdf

[11] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," Communications Surveys Tutorials, IEEE, vol. 11, pp. 42-56, Fourth 2009.