IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 8, Issue.5, May 2020 E-ISSN: 2347-2693

File Sharing Techniques in Digital world

J. Kanimozhi[1*], V. Swathilakshmi[2], S. Aravindh[3], S. Hemachandira[4], M. Dinesh[5]

[1,2,3,4,5]Dept. of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India

[*]*Corresponding Author: janathakani@gmail.com, Tel.: 7373231828*

DOI: https://doi.org/10.26438/ijcse/v8i5.149154 | Available online at: www.ijcseonline.org

Received: 10/May/2020, Accepted: 18/May/2020, Published: 31/May/2020

***Abstract*—** File sharing is the exchange of computerized data for example computer programs, audio or video records, documents or electronic books over the web with others. There are many ways of file sharing. Some of them are, Peer-to-Peer, Cloud storage service and Removable storage media. Peer-to-peer involves computer hardware and software to communicate without the need for a central server. Cloud storage service is like peer-to-peer file sharing. Notwithstanding, rather than sending the document straightforwardly to the others, the record is sent to a server that stores the record. When the document is put away in the cloud (on the web), we can allow different clients can download it by providing them the link of file. Removable storage media is vast different from other two ways. File sharing is done physically by the user with the help of any storage devices. In this work, we are going to see the different file sharing techniques used in this digital world.

***Keywords*—**File sharing, digital information, Peer-to-Peer files sharing, Cloud services, Removable storage media.

I. INTRODUCTION

File-sharing applications permit the clients to upload files to a common storage space and assign who may get to the files.

It is the public or private sharing of computer data or space in a network with different degrees of access benefit. While files can easily be shared outside a network, the the term document sharing about consistently implies sharing records in a network, even if in a small local area network. Document sharing permits various people to utilize a similar record or document by a mix of having the option to peruse or see it, write to or change it, duplicate it, or print it. Ordinarily, a document sharing framework has at least one administrator. Clients would all be able to have the equivalent or various degrees of access benefit. Record sharing can likewise mean having an allotted measure of private document stockpiling in a typical record framework.

Work environment record sharing applications goes under two significant gatherings: consumer and business grade. Buyer applications, (for example, Dropbox and Google Drive) are cloud-based and offers essential coordinated effort apparatuses, for example, record sync, stockpiling and sharing. Essentially intended for individual use by customers, these applications are reasonable (some are free) and highlight easy to use interfaces, yet regularly do not have the controls, security and oversight highlights of business applications. Business file-sharing software tend to offer more protection and enforcement functionality for corporate content management, such as automated workflows, document monitoring. Cloud computing is the provision of on-demand computer system resources, in particular data storage and computing power, without direct, active management by the customer. In general, the term is used to describe the data centers that are accessible over the Internet to many people.

The eventual fate of registering is in the cloud. It suggests that you adjust your business to fit in the cloud model. The inverse additionally remains constant as your business can be abandoned if this new innovation is underutilized or not used. Cloud computing models have three sorts of administrations: SaaS (Software as a Service), IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). Each model has their own arrangement of favorable circumstances that could serve needs of different organizations. When you pursue cloud administration models, you can use its more extensive prospects to bring the adaptability that pushes your business development.

Cloud storage isn't only for your own documents. You can utilize it to effectively share records with no challenges. Offer documents with your companions and partners, or make them accessible to the whole Internet. Common records can naturally synchronize to every individual's PC, or you can get to them through the web or versatile application. It is an advantageous method to share records than messaging them to and fro.

A cloud application is an Internet-based program where a portion of the processing logic and data storage is handled in the cloud. The client communicates with the application by means of program or versatile application, and a mix of the nearby PC and a distributed computing framework deals with the information preparing. From the client's point of view, the cloud application acts like a standard

site, yet the figuring and information preparing are dealt with by the cloud by means of API or a half breed of both. The cloud storage service resembles peer-to-peer sharing of data. The file is uploaded at the server that stores the file, instead of sending the files directly to the other user. Once the file is saved (online) in the cloud, others will be able to download the file if they have a connection to it. It offers end-users the way to access files from everywhere with any Internet-capable device. As a rule, the client can allow access to different clients from their perspective.

Despite the fact that cloud record sharing administrations are anything but difficult to utilize, the client needs to depend on the capacity of the specialist co-op to give auspicious, high accessibility and reinforcement and recuperation. It additionally offer high speeds to download records, speeds a typical client probably won't have the option to help (P2P document sharing paces are topped by your transfer transmission capacity). Utilize an online document stockpiling administration to have a similar record with different individuals, or offer a record later on with somebody and not transfer it once more. The document is kept as long as you need in your Cloud record stockpiling account.

Microsoft Windows is a network of Microsoft-produced working frameworks. Windows 10 presents the Universal Windows Platform (UWP), which furnishes any gadget running Windows 10 with a typical stage for the product. UWP center APIs are the equivalent for all gadgets running Windows. On the off chance that your product utilizes just the center APIs, it will run on any Windows 10 framework independent of whether you're focusing on a work area PC, Xbox, Mixed-Reality headset, and so on. UI components react to the size and DPI of the screen that the application is running on by altering their design and scale. UWP applications function admirably with various kinds of information controls, for example, console, mouse, tap, pen and Xbox One. In the event that you have to additionally redo your UI to a specific screen size or gadget, new interface boards and tooling can help you in structuring UIs that can change in accordance with the various gadgets and structure factors on which your application may run.

Android is a mobile operating system built on a modified version of the Linux kernel, as well as other open source software specifically designed for mobile devices such as smartphones and tablets. Android is developed by a group of developers known as the Open Handset Alliance, with Google being the principal contributor and marketer. The current stable version is Android 10. The main source code for Android is known as the Android Open Source Project (AOSP), which is published exclusively under the Apache licence. This has allowed Android variants to be built on a range of other devices, including game consoles, digital cameras, PCs and others, each with a different user interface.

In this paper the section II explains about the different file sharing techniques used in this digital world. Section III gives the conclusion of this paper by giving the pros and cons of the file sharing techniques.

II. FILE SHARING TECHNIQUES IN DIGITAL WORLD

File sharing involves data or space sharing in a network with different levels of privilege of access. Although files can be easily shared outside of a network, the term file sharing almost always means sharing files in a network, even if it is a small network of local areas.

There are different ways and applications to share a file and the applications are implemented using different technologies and methods. Here the file sharing methods are categorized based on the middle-ware present between the two end systems. And they are listed and explained below.

- Peer-to-Peer
- Cloud storage service
- Removable storage media

A. Peer-to-peer

Peer-to-peer networking involves computers to communicate without the need for a central server. This method of sharing of files suggests the location of digital files on a P2P network where the files are stored on one section of the device and shared with other users rather than on the server. In this, large files are broken down into smaller chunks which the receiver may obtain from multiple peers and then reassemble. This is done while the peer uploads chunks that it already has to other peers at the same time. Figure 1 shows the file sharing in a peer – to-peer method.

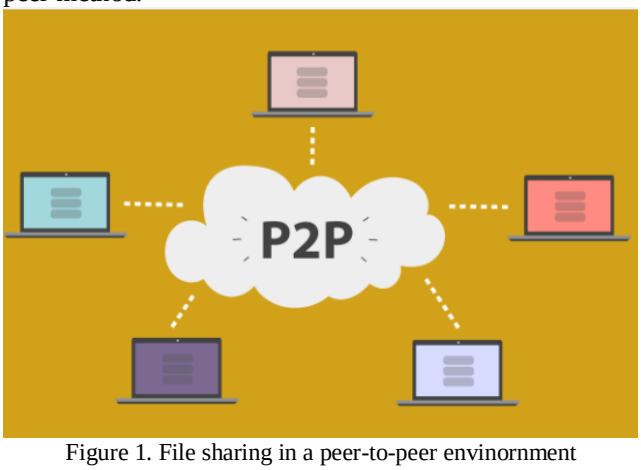

Figure 1. File sharing in a peer-to-peer envinornment

In [1], a P2P document sharing framework clarified and it comprises of two sections: search algorithm and a file transfer protocol. file transfer protocol is answerable for downloading documents by utilization of TCP connection. In this way scan algorithm is answerable for the transmission and search results of query messages. Also,

more consideration is attracted to the search algorithm, which has more connection with productivity.

As of late, there has been a hazardous development in the utilization of the distributed (P2P) frameworks. In [2], P2P are broadly utilized in file sharing applications, for example, BitTorrent. Over half of the files downloaded and 80% of the files transferred on the Internet are through P2P systems. P2P file sharing frameworks pull in a large number of clients. The compelling area of an ideal document has been an open issue for a long time, because of the enormous size of the P2P systems.

The BitTorrent (BT), most outstandingly, has made gigantic progress among Internet clients. In [3], Haiyang et al for the first time look at the difficulties and possibilities of quickening distributed file imparting to twitter interpersonal organizations. They introduced the companions in such swarms have more grounded transient territory, subsequently offering incredible open door for improving their level of sharing. In view of the Hadamard Transform of friends' online practices, they built up a social record to rapidly find companions of normal examples. Furthermore, they further showed a pragmatic collaboration convention that identifies and use the social relations with the list.

In the case of file sharing in wearable devices with PAN, the security of a file stored in it is an important concern. Traditional secret sharing has enormous overhead computing and requires a large storage space, and is not ideal for wearable devices powered by batteries. Combinatorial-based file sharing is proposed to overcome this problem. But even in this there is an efficiency problem, as preparation of file storage and retrieval involves computational costs. So in [4], Jung-Eun et al proposed a new algorithm that generates file shares by considering the heterogeneous characteristics of wearable devices. They considered the factors of storage capacity and network speed to determine the sizes of the file shares.

There are numerous kinds of P2P frameworks, which can be classified into two classifications:

- Unstructured
- Structured

1) Unstructured p2p system

For unstructured P2P frameworks, there is certainly not an organized overlay network among peers, for example Napster, Gnutella and Freenet.In [5], Napster has a concentrated server to store all keys of shared files. It's somewhat similar to the client server model in the sense that to provide directory support, it retains a massive central repository At the point when a peer sends a file inquiry, the file-query message is first sent to the unified server to find which peer claims the ideal file. At regular intervals, the server queries peers to ensure that the peers are still connected or not. Then, the desired file is downloaded from the found peer. So this server essentially maintains a huge database over which file is present at which IP addresses. Napster has the single point of failure problem, due to the centralized server. If the server fails, then the entire P2P network will crash. Therefore, since all processing must be performed by a single server, a huge amount of database must be maintained and updated regularly.

For other unstructured P2P frameworks, the file query is performed by a basic flooding system. Gnutella was the principal decentralized distributed system. At the point when a peer gets a file-query message, on the off chance that it has the ideal file, it will send back the file substance. Else, it just floods the file-query message to all its neighboring peers, i.e. to all nodes that are connected to this node. If those nodes do not have the file, they pass the query to their neighbors, and so on. This is called flooding by email.

In [6], they proposed a speculation of the essential flooding scan procedure for decentralized unstructured shared (P2P) systems. In their algorithm a peer will send an inquiry to one of their neighbors utilizing a likelihood that is a component of the number of connections in them two's overlay network. What's more, this probability may likewise rely upon the good ways from the query originator.

2) Structure p2p system

In the unstructured P2P frameworks if there are numerous peers, the flooding system may create countless file-query messages. In such case, the adaptability issue is presented. In [5], to counter the versatility issue, the structured P2P frameworks use the conveyed hash table to sort out peers into an organized overlay network, for example CAN, Chord, Pastry and Tapestry. The key to a shared file is stored in certain P2P systems in the peer whose node identifier is 'nearest' to the key. From that point, the execution of a file query resembles the capacity of finding out which peer is answerable for putting away the key of the common file. Not at all like the unstructured P2P frameworks, the file-query message can be ensured inside O(logN) consistent logical hops to the peer with the file key, where N is the absolute number of peers in the P2P framework.

To think about the physical network topology and the heterogeneity in the assets of peers, the peers in the unstructured or organized P2P frameworks can be additionally sorted out into a various hierarchical architecture. Super-peer-based P2P frameworks are designed both flooding and concentrated level design. The peers in a super-peer-based P2P framework are separated into two sorts: super-peer and regular peer. The super-peer is a high-ability hub that goes about as an incorporated server to serve a gathering of regular peers whose whose geographical locations are neighboring one another.

B. Cloud storage service

With the dangerous development of the web, putting away the sheer measure of information locally is a substantial

weight for clients. So an ever increasing number of associations and people need to store their information in the cloud. In any case, the information put away in the cloud might be undermined or lost because of the cloud's unavoidable programming bugs, equipment flaws and human blunders. So as to check whether the information is put away accurately in the cloud, numerous remote information trustworthiness evaluating plans have been proposed [7]. In many cloud storage frameworks, for example, Google Drive, Dropbox and iCloud, the information put away in the cloud is regularly shared by various clients. Information sharing as one of distributed storage's most regular highlights permits various clients to impart their information to other people. Figure 2 shows the file sharing method using cloud.

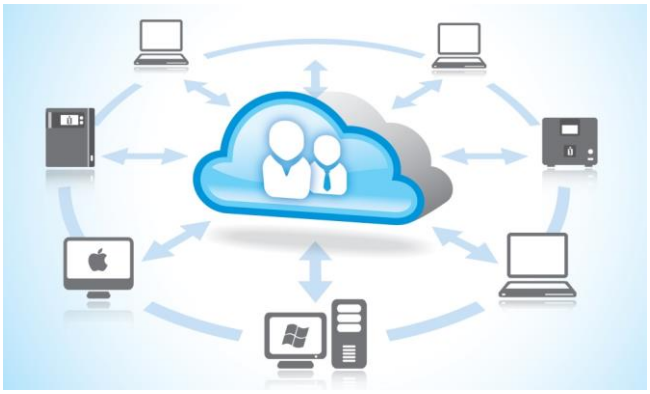

Figure 2. File sharing through Cloud

Cloud storage administration is like peer-to-peer peer-to-peer record sharing. As opposed to sending the document legitimately to the next individual, nonetheless, the record is sent to a server which stores the record. When the record is put away in the cloud (on the web), others can download the document on the off chance that they have a connect to the document. It furnishes end clients with the capacity to get to records with any Internet-competent gadget from any area. The client normally can allow different clients get to rights as they see fit.

In spite of the fact that cloud document sharing administrations are anything but difficult to utilize, the client needs to depend on the capacity of the specialist organization to give opportune, high accessibility and reinforcement and recuperation. It additionally offers high speeds to download documents, speeds a typical client probably won't have the option to help (P2P record sharing velocities are topped by your transfer data transfer capacity). Utilize an online file storage service to have a similar record with numerous individuals, or offer a document later on with somebody and not transfer it once more. The record is kept as long as you need in your cloud file storage account.

But there are concerns with valuable and important data being stored remotely. Once you implement cloud technology, you should be mindful that you are supplying a third-party cloud service provider with confidential business information and this could potentially put your organization at risk or there may be a vulnerability to external hack attacks. The internet is not completely secure, and for this purpose, sensitive data can always be stealthy.

A potential strategy for tackling this issue is to scramble the entire shared file with the client key before sending it to the cloud, and afterward create the marks used to confirm the honesty of this encoded file, finally transfer this encoded file and its relating marks to the cloud. This strategy can understand the sensitive data covering up since just the information proprietor and the client can decode this file. What's more, it will make the entire shared file unfit to be utilized by others. Just with the client key, the information can be decoded to the ordinary record.

In [8] DaSCE was proposed with Semi-Trusted Third Party, an information security structure offering (a) key administration (b) access control, and (c) ensured cancellation of data. The DaSCE utilizes Shamir universal threshold scheme (k, n) to deal with the keys where k is expected to create the key out of n shares. They utilized different key supervisors, each facilitating one portion of key. For cryptographic keys numerous key supervisors forestall a solitary purpose of disappointment. Their outcomes uncovered that DaSCE can be adequately utilized for security of redistributed information by utilizing key administration, get to control, and ensured cancellation of the document.

In [9], they proposed two possible instantiations of the shared ownership model. First approach, called Commune, is focused on safe file dispersal and collusion-resistant secret sharing to ensure that all cloud access grants require an agreed owner's threshold to be accepted. Second solution, called camarade, leverages the blockchain technology to reach consensus on decision on access control.

It is important to have cryptographically enhanced access control mechanism on the common data for secured sharing of files. Identity-based encryption is a promising basic cryptography for developing a functional data-sharing network. Access control isn't static however. That is, the point at which the approval of certain clients is terminated, a procedure ought to be set up that can erase them from the network. Thusly, the renounced client cannot get to the mutual information, both beforehand and in this way. Thusly, in [10], they presented an idea called revocable-capacity personality-based encryption (RS-IBE), which can give forward/in reverse ciphertext insurance by all the while executing client denial and ciphertext update functionalities. Also, we present a solid RS-IBE development and demonstrate its assurance in the given model of protection.

In [11], Danan et al introduced SafeProtect which packages the information proprietor's information and approach, in view of XACML, in an object. SafeProtect implements the approaches set by the information proprietor to impair

those commands and additionally run a foundation procedure control for auditability/responsibility purposes, by collaborating with the SaaS customer. They defined a convention that will empower secure information partaking in the Cloud and influence the utilization of the Trusted Extension Device (TED) for confirmation purposes

Steganography role to provide security in e-commerce transaction is given in [12]. In which the data is transferred through internet and by using the steganography the data is secured. Marripelli Koteshwar explained the security issues in data sharing in [13]. In [14] Shailja Sharma has shown the cloud security performance. Traffic is a very important thing in file sharing through cloud. How to coltrol network traffic using AI is explained by N. Selvakumar in [15]. Data is fetched from cloud using mobile application namely javabot and notybot in [16] [17] by J. Kanimozhi et al.

C. Removable storage media

It includes anything from a system or computer that can be removed. The user may transfer or move files from their computer to the removable storage media and then hand them physically to whomever they wish to share the files Those may include a security-related FTP server asking others for a valid username and password to allow access. Figure 3 shows the removable storage media to share file.

Figure 3. File sharing through removable storage media

Utilizing a low entropy secret phrase, customer storage devices are normally made sure about to oppose unapproved get to. Regardless, capacity gadgets are not completely secured against an adversary in light of the fact that the rival may utilize a disconnected word reference assault to locate the right password or potentially execute a current algorithm for resetting the current password. So, in [18], they proposed a shared mutual authentication and key negotiation protocol that can be utilized to ensure the protection of confidential data stored in the device. The protocol structure makes the storage device protected from potential security assaults.

1) Moving or delivering large amounts of data: If you need large amounts of data to be transported or stored, the best solution is often an external or disposable hard disk. External hard drives in very high capacity are available. A removable hard drive device frame/carrier utilizes standard hard drives, as is constrained in volume just by the size of the biggest accessible standard hard drives.

2) Information backup: Tape drives, optical drives, and other conventional backup arrangements are excessively slow and have too little ability to be commonsense for doing finish reinforcements of the present huge hard drives. What's required is something that is quick, stores a ton of information, and doesn't cost much per byte put away. As it were, a hard drive. Notwithstanding their speed and limit favorable circumstances, removable hard drives have a significant bit of leeway on the off chance that you experience catastrophic framework failure, since you can just associate the reinforcement hard drive and boot it straightforwardly, without investing the energy expected to revamp the framework, reinstall the working framework and applications, and recover from tape.

3) Offline data storage: Indeed, even the biggest hard drive, especially in case a pack rodent like Robert, will in the long run fill in. External or removable hard drives permit boundless measure of offline information to be stored. For instance, one of our perusers tore his whole assortment of DVD films to a few external hard drives, and securely stored the original disks. Every external drive store somewhere in the range of 40 and 100 motion pictures, contingent upon the drive's ability, the size of the films and the compression level he utilized while tearing the motion pictures. He has a pivoting determination of a few of these outside hard drives connected to his home-theater PC, and consistently has a choice of 100 to 250 motion pictures accessible for guaranteed screening basically by choosing from a catalog listingIf a film that he needs to watch is on a disconnected drive, it just takes seconds to connect that drive and access the video. Others utilize outer or convenient hard drives to store records, computerized pictures or home video libraries. One person we know tracks his preferred TV appears for an entire season, spares them to outside hard drives and rehashes them in a long-distance race meeting after the season is finished.

Securing information: On the off chance that you utilize an outer or dispensable hard drive to work with incredibly delicate information, for example, finance records, you can ensure the information by taking it with you or putting away it in a safe.

III. CONCLUSION AND FUTURE SCOPE

In removable storage media, the file sharing is done physically by the user with help of storage devices. It is the out-dated type of sharing the file. In this, the user has to manually copy the file to storage device and transfer the device to other user physically. It is a time-consuming process to do it manually. So, there comes the other two ways of file sharing P2P and Cloud service.

In P2P, the devices should be in the same network for the file transfer. Computers connected via a Wireless Local Area Network, can transfer files over the network to other connected computers. Whereas in cloud service, it is not necessary that the devices should be in same network. If we have internet facility, we can easily share file to others by uploading it to the cloud storage and share the link. From the above analysis, it is concluded that file sharing using cloud service is better than other two.

Even though the cloud service has major advantage in sharing file between the users in larger distance are also some security break through. To solve this security issues, there are many work and implementation of new protocols are going on.

REFERENCES

[1] Bhagat, A., Chaudhari, R., & Dongre, K., "*Content based File Sharing in Peer-to-peer Networks Using Threshold*", Procedia Computer Science, 79, 53–60, 2016.

[2] Shen, H., Li, Z., & Chen, K., "*Social-P2P: An Online Social Network Based P2P File Sharing System*", IEEE Transactions on Parallel and Distributed Systems, 26(10), 2874–2889, 2015.

[3] Wang, H., Wang, F., Liu, J., Lin, C., Xu, K., & Wang, C., "*Accelerating peer-to-peer file sharing with social relations*", IEEE Journal on Selected Areas in Communications, 31(9),66–74, 2013.

[4] Park, J. E., & Park, Y. H., "*Fog-based file sharing for secure and efficient file management in personal area network with heterogeneous wearable devices*" Journal of Communications and Networks, 20(3), 279–290, 2018.

[5] Lin, J. W., & Yang, M. F., " *Robust super-peer-based P2P file-sharing systems*" Computer Journal, 53(7), 951–968, 2010

[6] Gaeta, R., & Sereno, M., " *Generalized probabilistic flooding in unstructured peer-to-peer networks*", IEEE Transactions on Parallel and Distributed Systems, 22(12), 2055–2062, 2011.

[7] Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J., " *Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage*", IEEE Transactions on Information Forensics and Security, 14(2), 331–346, 2018.

[8] Ali, M., Malik, S. U. R., & Khan, S. U., "*DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party*", IEEE Transactions on Cloud Computing, 5(4), 642–655, 2015.

[9] Ritzdorf, H., Soriente, C., Karame, G. O., Marinovic, S., Gruber, D., & Capkun, S., "*Toward shared ownership in the cloud*", IEEE Transactions on Information Forensics and Security, 13(12), 3019–3034, 2018.

[10] Wei, J., Liu, W., & Hu, X., "*Secure data sharing in cloud computing using revocable-storage identity-based encryption*", IEEE Transactions on Cloud Computing, 6(4), 1136–1148, 2018.

[11] Thilakanathan, D., Chen, S., Nepal, S., & Calvo, R., "*SafeProtect: Controlled Data Sharing with User-Defined Policies in Cloud-Based Collaborative Environment*", IEEE Transactions on Emerging Topics in Computing, 4(2), 301–315, 2016.

[12] S. Bansal, "*Data Security by Steganography: A Review*", International Journal of Scientific Research in Network Security and Communication, Vol.7(1), Apr 2019.

[13] Marripelli Koteshwar, Bipin Bihari Jaya Singh, "*Survey Report on Cyber Crimes and Cyber Criminals Get Protected from Cyber Crimes: Review Paper*", International Journal of Scientific Research in Computer Science and Engineering, Vol.7, Issue.6, pp.46-56, 2019.

[14] Shailja Sharma, Sheeba Khan, "*Analysis of Cloud Security, Performance, Scalability and Availability (SPSA)*", International Journal of Scientific Research in Network Security and Communication, Volume-7, Issue-1, 2019.

[15] N. SelvaKumar, M. Rohini, C. Narmada, M. Yogeshprabhu, "*Network Traffic Control Using AI*", International Journal of Scientific Research in Network Security and Communication, Vol.8, Issue.2, 2020.

[16] Kanimozhi.J, Balla Sri Satya, Dharni Pryanka.S, Susela .J, " *Javabot - Chatterbot Using Java to Assist Healthtip, Share market and Sports Updates*", International Journal of Application or Innovation in Engineering & Management, Volume 8, Issue 4, 2019.

[17] J. Kanimozhi, V. Swathilakshmi, P. Bhavani, V. Vijayalakshmi, "*NOTY BOT - A Personal Assistant that Integrates the Updates*" , Information Technology & Electrical Engineering, vol 9, issue 1, 2020.

[18] Amin, R., Sherratt, R. S., Giri, D., Islam, S. H., & Khan, M. K., "*A software agent enabled biometric security algorithm for secure file access in consumer storage devices*", IEEE Transactions on Consumer Electronics, 63(1), 53–61, 2017.

Authors Profile

MS. J. Kanimozhi pursed B.Tech (IT) at Pondicherry Engineering College and M.Tech (CSE) at Pondicherry University, Puducherry, India. Currently working as an Assistant Professor in Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. Her area of interest is Computer network Security, Evolutionary Algorithms and Android Application. She has 2 years of teaching experience.

Ms V. Swathilakshmi pursed B.Tech CSE and M.Tech (CSE) from Pondichery University and Currently working as an Assistant Professor in Department of Computer Science and Engineering, Sri Manakula Vinayagar Engineering College, Puducherry, India. Her area of interest is DBMS, Android Application. She has 2 years of teaching experience.

S. Aravindh pursing B.Tech (CSE) at Sri Manakula Vinayagar Engineering College, Puducherry, India. His are of interest is web development and Android application development.

S. Hemachandira pursing B.Tech (CSE) at Sri Manakula Vinayagar Engineering College, Puducherry, India. His are of interest is web development and Android application development.

M. Dinesh pursing B.Tech (CSE) at Sri Manakula Vinayagar Engineering College, Puducherry, India. His are of interest is web development and Android application development.

