International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

SECURE FILE SHARING AND RETRIEVAL USING FOG NODES

Asha Elsa George[1], Ajeesh S[2], Smita C Thomas[3]

[1]P G scholar, Dept. of CSE, Mount Zion College of Engineering, Kadammanitta, Kerala, India
[2]Assistant Professor, Dept. of CSE, Mount Zion College of Engineering, Kadammanita, Kerala, India
[3]Research Scholar Vels University, India

Abstract - *The surveillance of data accumulation is an essential burden in personal area network. Secret allocation has earned appreciable scrutiny for manipulating surveillance. The fog nodes also assures the clandestineness, rectitude alike although a few gadgets. If the count taken together less than the minimum verge, then negotiate, adrift or lifted. To overcome the introductory problems, a fog node that delegate the estimation for the scheduling of file sharing, file cache and convalescence. Fog network model has approximately agile useful appropriateness and has larger battery space. The device assets in personal area network with wearable devices will be accurately handled and a proxy re-encryption scheme is used to improve confidentiality and security.*

Key Words*:* Storage, Fog computing, PAN, Secret sharing, Proxy Re-encryption

1. INTRODUCTION

The assessment and communication applications in wearable resources are more desirable along with normal to augment information and also, the administration of wearable devices is rising tremendously [1]. This device does not collect the stored files from the wearable resource. It transmits the message to remote servers through internet and can exchange the stored data throughout the PAN. When the devices are connected to other wearable resources through PAN, the accumulation of secluded files may be dispersed to alternative devices. In such organizations, secretiveness of delicate information should be endorsed. If the virtue and availability of such file is not treated, a wearable device may create a erroneous interpretation or a fraudulent consequence. PAN devices are luminous, minuscule, and convenient, accomplish them decumbent to damage or piracy. In such cases, the gathered file can be cracked or disoriented forever [1]. The quantities of estimation along with depot of a like devices are fewer than that of legitimate computers and thus the preservation applications equipped in such devices in a PAN afford a curtailed level of surveillance. Appropriately, the devices are decumbent the scheduling. To overthrow the introductory complications, a furtive allocation strategy will be endorsed for assuring the decisive files.

The furtive distribution is an arrangement that disciple a private expense to considerable stake, where a part or all of them can reclaim the authentic obscure value. Occasionally, the aforementioned strategy is called as (r, a) –secret sharing or (r, a) –verge, where a is the number of all the established contribution and r is the minimum number of shares that can reclaim the authentic secluded. The furtive researchers admit its advanced transcription subsequently. A Scheme that contain a device in the PAN, and at least r devices are needed to retrieve the original data.

In the file bury operation, a device that tries to deliver a file first creates a file allocation strategy was independently assorted shares using the secret sharing scheme. Subsequence that, the device manage one amid authority and assign the other a-1 contribution to the a-1 devices, respectively. In the file recapturing operation, a mechanism that tries to consignment a file from the PAN, first chooses a –1 device, and then appeal them to commit their own file stakes. The gadgets to reclaim the authentic file using the received r – 1 file shares and its own contribution.

Surveillance susceptibility and concealment abuse by malicious attackers or internal users can arise from various types of data transactions. The discern file is digitized and gathered by a centrally managed detective in the data intermediary, if it is inadequately used by the user, it can lead to a contravention of the original concealment. Accordingly, accurate for astute preservation to be stimulated, it is decisive to persuade the confidentiality of shared file and to protect the access rights. In this paper under which encrypted file are decrypted using a proxy based re-encryption strategy, the actual furtive pivotal is not dispersed.

The conveyance is adequate to decrypt adopting the re-encrypted obscure pivotal. This authorization of claim will clarify the controversy in protected appropriation and utilization of information when the information is being handled.

2. RELATED WORKS

Cloud computing is an auspicious automation, which is altering ordinary Internet enumerate prototype. With the advancement of wireless approach automation, cloud computing is normal to enlarge to mobile status, where sensors are used as the information assemblage burl for the cloud. The user's crisis about file surveillance is the needed regulations that retard cloud computing from being extensively managed. These burdens are commenced from the element that sensible information located in public clouds that are negotiated by monetary utility providers that are entrusted by the file owners. So, advanced protected

utility architectures are desired to detect the preservation concern of users for cloud computing efficiency.

In this paper, surveillance frame work to assure the information rectitude in public clouds with the appropriate target on incompetent wireless devices store the data and recapture file without displaying the file satisfied to the cloud service providers. To accomplish this target, solution targets on the following two methods for secure file sharing and retrieval. First, a novel Privacy Preserving Cipher Policy Attribute Based Encryption to protect user's data [8]. PP-CP-ABE is used in incompetent devices can vigorously redistribute heavy encryption and decryption transactions to cloud service providers, beyond affirm the data comfortable and used surveillance keys. Second, an Attribute Based Data Storage system as a cryptographic approach authority contrivance. ABDS accomplish data analytical optimality in reducing estimation, cache and computational overheads. Exclusively, ABDS reduces cloud service allegation by reducing transmission overhead for data managements.

3. EXISTING SYSTEM

Distributed storage shows a decisive aspect in the network of personal devices, owing to its fault tolerance and quick retrieval of stored files. To augment the surveillance and concealment of the gathered information. Secret distribution strategy has been employed for allocating storage. Among the existing secret sharing schemes, a combinatorial-based file distribution strategy is more convenient one because of its incompetent frame work and low cost [8]. However, there remains the problem that the capacity of the distributed stored file contribution in devices does not support the heterogeneous personal device environment, which may cause an additional efficiency problem. In this paper, provide a competence- augment combinatorial-based file distribution strategy for distributed storage with personal devices, which deals with the amalgamate aspect thereof. In addition to actual combinatorial-based file distribution strategy, for the file bury mechanism, a method for find the capacity of file contribution according to remaining depot capacities, average communication speeds of the participant personal devices. In the discussion, we demonstrate that our scheme manages the distributed storage system with personal devices efficiently compared to alternative existing sharing schemes [7].

Fig 3.1 describes the file repository process. Let the gadget that establish an advanced file and endeavor to store it to the dispersed repository be a **creator**, which is represented as a pair of smart glasses in the figure [3.1].

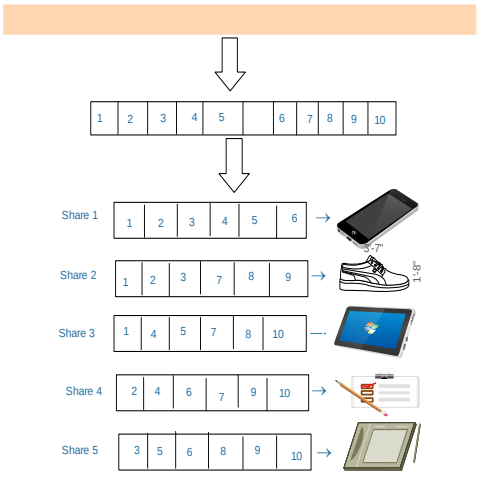

Fig 3.1 Combinatorial based file sharing- Storage

When the creator delivers the file to the dispersed system, it first creates *a* file contribution. For this, the creator handling the subsequent operations: the creator regulates the capacity of a file contribution by considering the amalgamate aspect of the member devices. Consecutive this, the creator partition the authentic file into (ar−1) files. Definitely, the creator achieves a file contribution by reassembling the file sections. Note that each file contribution is composed of (a−1r−1) segments, and that any r among the *a* file contribution encompass all of the (ar−1) files section, but any r−1 among a do not.

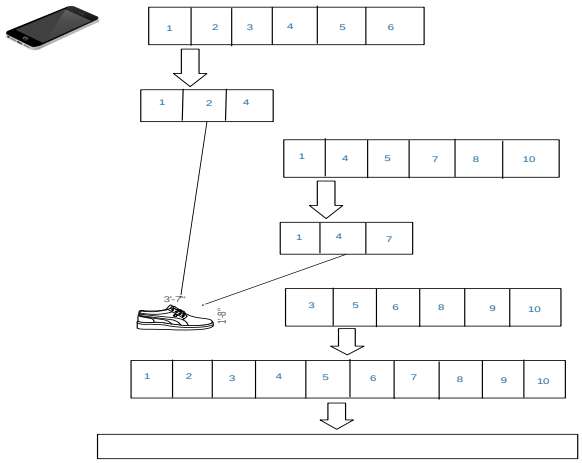

Fig 3.2 Combinatorial based file sharing- retrieval

Fig 3.2 describes the process of file convalescence from the dispersed repository. In this mechanism, let the gadget that endeavor to reclaim the file gathered in the dispersed repository be a **collector**, which is represented as a smart phone in the figure. To reclaim the authentic file, a file contribution must be possessed; so, the collector desires that a −1 devices dispatch a file contribution to the collector. In this study, does not address schemes of nominating the r−1 of the a−1 devices. To reclaim the file, the collector may obtain r−1 file contribution from the r−1 devices to assemble

r file shares. Yet, replicated file segments endure in the r shares. The correspondence of the digitized details from the r−1 devices should be the similar as that of the transmission agility between the collector and the r−1 devices. If this is prohibited, a device with curtailed transmission agility may issue large parts of its own file share to the collector. The download scheduling algorithm regulates the element capacity of each file segment that the collector downloads from the r−1 devices. After using the algorithm, the collector delivers the solution to the r−1 devices, and the devices circulate back the parts of the file sequences to the collector. Finally, the collector fetches the original file on completion of the transmission [8].

4. PROPOSED SYSTEM

The comprehensive exemplary of the fog-based (r, a)−file contribution strategy for the PAN. The PAN dwells of battery-mechanized devices with insignificant gauge capability and defined assets such as wearable devices. Despite the (r, a)−file contribution strategy diminish the computational aloft for achieving the file contribution and recapturing the authentic file, the operations for finding the capacity of the file contribution and organizing the load may be a burden on the devices because they consist of a few complicated process.

Auspiciously, there is an approximately authoritative gadget that has larger battery space and can appraise agile than the rest. Accordingly, the transaction can be authorizing to the smart phone.

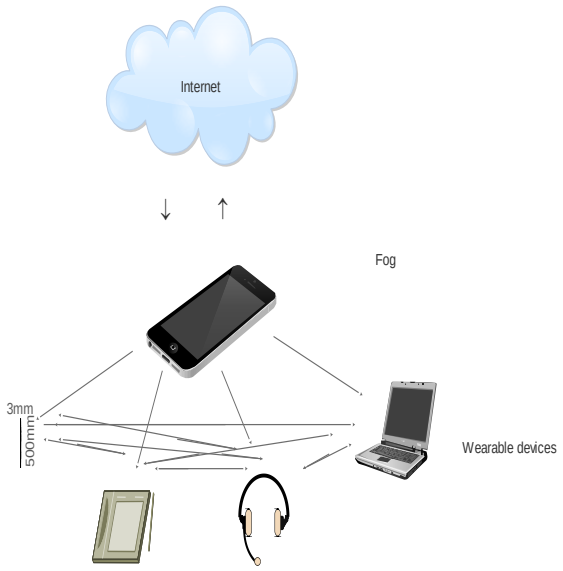

Fig 4.1 Fog model based on PAN

To gadget this strategy, afford a fog-based PAN with wearable devices. A fog node in the form of a smart phone is coeval in between the internet and PAN. In alternative contention, there are three layers delineated in Fig 4.1. The lowest layer normally subsist of wearable devices with smaller enumerate power and finite assets; the peculiarity of devices like convenient capacity or bandwidth are diverse. Assume that when each pair of devices is linked, each device is linked with the fog node. The intermediate layer is a fog node whose aspiration is being accredit to the complex estimation and associating the wearable devices and the internet. Fog node recognizes the tendency of the wearable devices and communication speed between each pair of devices. Finally, the fog replace sends the *a* shares to the *a* devices, respectively.

4.1 PROXY ASCRIPTION STRATEGY

Proxy re-encryption strategy disciple the cipher text so that the intermediary can adopt Bob's furtive decisive to decrypt the cipher text, which antiquated encrypted with Alice's public key.

The intermediary can adherent the cipher text without decrypting the actual cipher text by using the re-encryption key to disciple the cipher text, the proxy appreciate neither the plaintext nor Alice's secret key. This approach can be prescribed to the conveyance of encrypted mail, file systems etc…

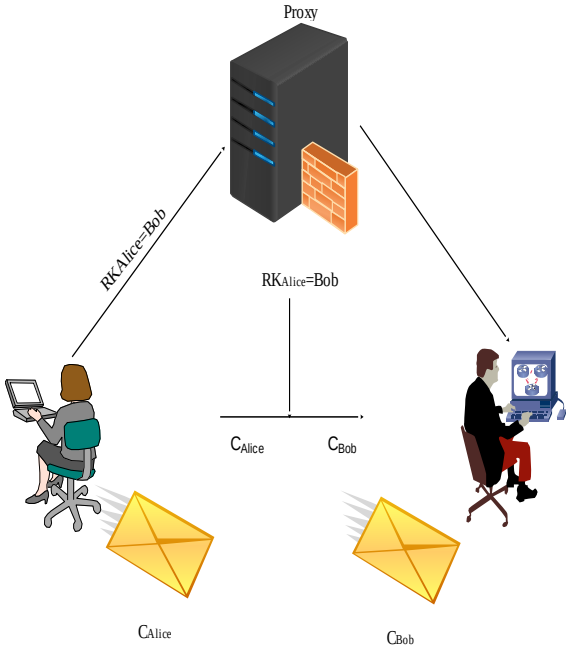

Fig 4.2 Proxy ascription strategy

Proxy re- encryption schemes are indistinguishable to conventional symmetric or asymmetric encryption strategies, with the addition of two functions:

- DELEGATION

Delegation grants an information beneficiary or key holder to achieve a re-encryption key based on his secret key and

the key of the delegated user. This re-reincarnation key is used by the surrogate as absorption to the re-encryption function, which is accomplished by the proxy to translate cipher texts to the delegated users key.

- TRANSITIVITY

Transitive proxy ascription schemes grant for a cipher text to be re-encrypted an endless number of times.

5. CONCLUSION

Owing to the combinatorial-based file allocation strategy, the gathered file can be recaptured even when $a - r$ devices are adrift, stolen, or compromised. Furthermore, the data cannot be leaked even when k–1 devices are lost, filched, or negotiate. Additionally, correlated to preceding furtive allocation process, the combinatorial-based process does not handle complicated polynomial effort and favor the amalgamate aspect of the participant devices, thus translation it convenient for a wearable device environment. Moreover, in the proposed model, a relatively powerful device such as smart phone plays the role of fog node, which itinerary file repository and convalescence. Because the scheduling process that associates large aloft is negotiated by a fog node, the wearable devices reduce battery consumption. With the proposed scheme, the files can not only be gathered in the wearable devices securely and efficiently, but also can be loaded optimally. A Proxy re-encryption scheme is used to improve clandestineness and surveillance in data sharing.

REFERENCES

[1] E. Jovanov et al., "Patient monitoring using personal area networks of wireless intelligent sensors," Biomedical Sci. Instrumentation, vol. 37, pp. 373–378, 2001.

[2] E. Jovanov et al., "Patient monitoring using personal area networks of wireless intelligent sensors," Biomedical Sci. Instrumentation, vol. 37, pp. 373–378, 2001

[3] E. Jovanov et al., "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," J. Neuro Engineering rehabilitation, vol. 2, no. 1, pp. 6, Mar. 2005.

[4] S. Saleem, S. Ullah, and H. S. Yoo, "On the security issues in wireless body area networks," J. Digital Content Technol. Applicat., vol. 3. no. 3, pp. 178–184, Jan. 2009.

[5] S. Saleem, S. Ullah, and K. S. Kwak, "Towards security issues and solutions in wireless body area networks," in Proc. IEEE INC, Gyeongju, pp. 1–4, June 2010.

[6] Ameen et al., "Security and privacy issues in wireless sensor networks for healthcare applications," J. Medical Syst., vol. 36, no. 1, pp. 93–101, Feb. 2012.

[7] K. Kaur et.al," Container- as- a- service at the edge: Trade-off between energy efficiency and service availability at fog nano data centers," IEEE Wireless Communication, vol. 24, no. 3, pp. 48-56, June 2017.

[8] J. E. Park, B. Bold, and Y. H. Park, "Efficient scheme for generating file shares in combinatorial-based file sharing with distributed cloud storage," in Proc. ICGHIT, Hangzhou, pp.79–80, Feb. 2017.