An Efficient and Secured Secret Password Sharing Technique using Block Chain

Adury Vijay Kumar, Avvaru Anil Kumar, Kotra Mounica, Sambangi Hitesh

Abstract: ***It will be the age communication and information methodology. Novel methodologies are developing gradually. With the advancement of novel technologies, secret & private data are also expanding. Whether this dangerous data will to be shared then point it gets exceptionally troublesome to share this private &secure data. In this manuscript, centralization will be completed on emerging a method to share secret ID safely utilizing secret sharing method. The secret sharing method begins withsecret & then derives from it specific shares that are dispersed to clients. Consequently, in this manuscript, the technique will be exhibited through that secret ID might be safely disseminated to few clients. At necessary, the unique secret ID might be improved & utilized. Therefore, this manuscript gives a technique through that client might share data safely. From the evaluation &confirmation it will be establish that the algorithm provides reasonable outcomes.***

Keywords: Password authentication, Secret Sharing, Information Security.

I. INTRODUCTION

Cloud computing, cloud service, and mobile internet will be getting popular & getting developed gradually. They are very significant in our routine life. As the utilization of cloud & server are expanding, humans are being examined to store their private data on cloud through the internet. While human store their private data on the cloud, they assume that the providers of cloud service would protector & give safety to their information and providers is not interrupt their confidentiality. The possibility of information outflow will increases with the increasing the utilization of server storage & internet. On other hand, when the information being stored & managed in framework, the framework takes archive & information or copies it. These copies are significant for the networks & frameworks. Humans cannot have any knowledge of these copies, thus there are possibilities of outflow of their confidentiality. Whether other side will be deliberated, human's confidentiality might be leaked with the use of few service providers, hacker intrusion, and few legal actions.

Revised Manuscript Received on 30 March 2019.
***** Correspondence Author
Adury Vijay Kumar* , Department of Computer Science Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P.
Avvaru Anil Kumar, UG Students, Department of Computer Science Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, A.P.
Kotra Mounica, Sambangi Hitesh UG Students, Department of Computer Science Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, A.P.

II. DATA SECURITY METHODS

There are dissimilar data security methods& every technique has its benefits & confines. These techniques are explained below:

2.1 Encryption and Decryption

The encryption will be procedure of translating plain text into the cipher text. The plain text will be unencrypted data. To access cipher text, client should decrypt & retain in real form as the plain text. The data access privacy & confidentiality confirms privacy of data. There are 2 kinds of data encryption algorithms;they are asymmetric encryption & symmetric encryption. Asymmetric encryption will also recognize as public key cryptography. It utilizes 2 diverse keys that are statistically encrypted, one will be private & another will be public. The private key will be kept public & secret, and it will be exposed to all. In this encryption, both private & public keys might encrypt the message. The reverse key that will be utilized to decrypt the message by receiver & utilized to encrypt the message by sender and vice versa. This technique will be slow, however it gives privacy security. Symmetric encryption utilizes similar key to decrypt file or message. For data decryption, receiver wants to utilize key that will send of sender through encryption of data. This will be much quicker than asymmetric encryption.

2.2 Homomorphic Encryption

The homomorphic encryption permits client do difficult mathematical calculations or operations on the information without decrypting it. This encryption permits to do operations to authorized client not to other client. In cryptographic methods, client requires to decrypt information whereas accessing it that creates it vulnerable.

III. PROPOSED METHODOLOGY

Information Technology is referred as survey or utilization of computer and telecommunication system for storing, retrieving and sending information. Now a days, information technologies are used everywhere in the world. Government agencies, military departments, corporation, financial institution, hospitals and almost all private and public sectors collect a good deal of privatedata of their "products, users, employees, research and financial status". Almost all of the data will be now collected, managed and stored within

computer & transmitted across networks to other computer. So security of confidential information is a crucial aspect in the information technology. This manuscript, deliberation is completed on enhancing an algorithm to share secret ID safely utilizing secret sharing method, This secret sharing method begins with a confidential & then derives from it specific shares that are disseminated to clients. Thus, in this manuscript, the technique will be existed through that secret ID might be safely disseminated to numerous clients. While requirement, the real secret ID might be improved & utilized further. Therefore, this manuscript offers a technique through that client might share data safely.

Step 1. The secret ID will be generated.

Step 2. Secret key will be separated into n-segments for n clients (as per the necessity).

Step 3. Every segment of the secret ID will be encrypted.

Step 4. Encrypted segments together with real secret ID will be protected for upcoming utilization.

Step 5. Encrypted segments of secret ID will be disseminated to clients (one segment to every client).

Step 6. Currently whenever secret ID will be required to enter into protected framework, then every segment of encrypted secret ID will be required. Therefore, all clients should remember & should be existstheir secret ID.

Step 7. All segments of secret ID in enter into framework.

Step 8. All segments are authenticated with protected secret ID.

Step 9. Whether all segments matches & none of the segment will be lost.

The framework will be tested with dissimilar no. of segments & dissimilar length of secret ID. It will be also tested with dissimilar formats of secret ID. It represents that framework provides reasonable outcomes.

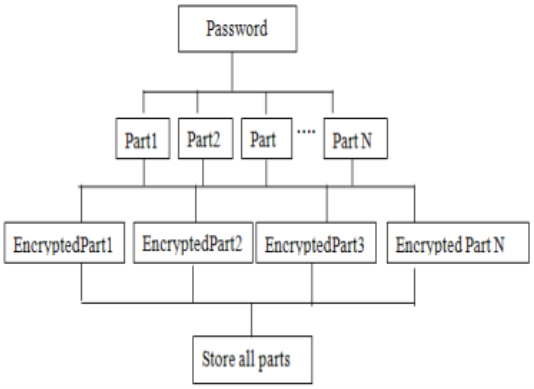

Figure 1. Creating encrypted parts of password

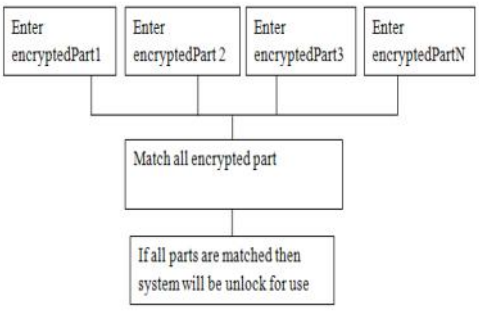

Figure 2. Unlocking system by entering encrypted parts of password

3.1 Algorithm

Sha-1 (Secure hash algorithm)

The message integrity algorithms confirminformation has not been modified in the transit. They utilize 1 path hash functions to identifywhether information has been modified. The Secure hash algorithm (Sha-1)is recognized as HMAC-Sha-1 will be a robust algorithm of cryptographic hashing algorithm, and it is stronger than MD5. Sha-1 will be utilized to offer authentication & data integrity. The sha-1 was generated to be utilized with standard of digital signature. Sha-1 utilizes a encryption key of 160-bit. It will be cryptographically stronger & suggested when higher safety required.

IV. RESULTS

Shown the below figure 3 secret sharing password technique

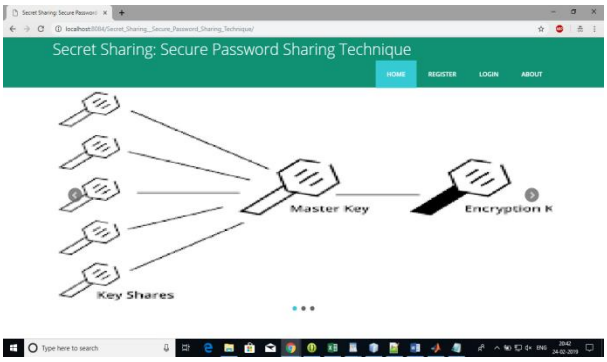

Figure.3.Secure Password Sharing Technique

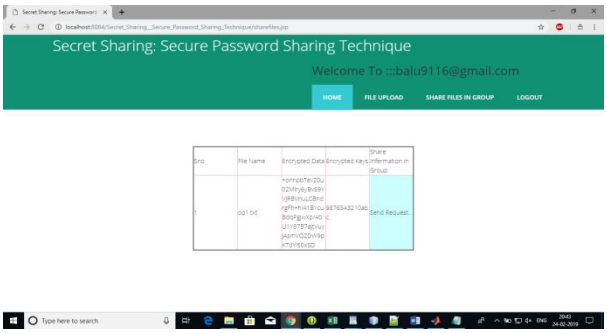

Figure.4. after sharing the password access

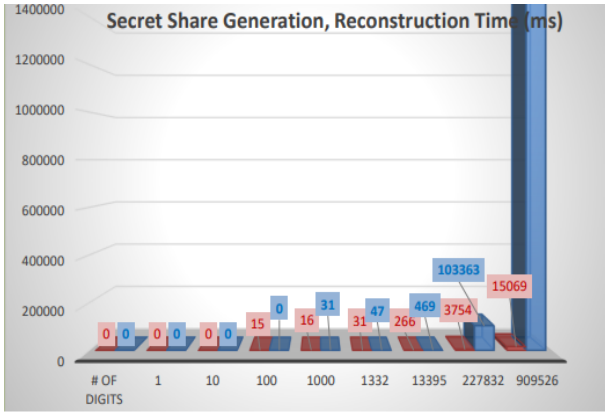

Figure.5. Sharing password various generations, Reconstruction time (ms)

V. CONCLUSION

In this manuscript, diverse techniques of data safety have been deliberated. The algorithms of data security have a many applications across diverse domains. In case, security of data over the cloud that might consist client's private pictures, account number, videos, and secret ID, so on. The Rabin's Information Dispersal Algorithm (IDA) and Shamir's Secret Sharing algorithm will be computationally low-cost than conventional cryptographic methods. These all methods do not need special ability hardware or they are not hardware dependent. By deliberatingabove facts, one might say that SeDasframework that offers extremesafety to data of client over cloud by utilizing Shamir's Secret Sharing Scheme Algorithm that will be most enhancedprocess.

REFERENCES

1. Geambasu, Roxana, et al. "Vanish: Increasing Data Privacy with Self-Destructing Data." USENIX Security Symposium. Vol. 316. 2009.
2. Shamir, Adi. "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.
3. Wolchok, Scott, et al. "Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs." NDSS. 2010.
4. Zeng, Lingfang, et al. "Safevanish: An improved data self-destruction for protecting data privacy." 2010 IEEE Second International Conference on Cloud Computing Technology and Science. IEEE, 2010.
5. Qin, Lingjun, and Dan Feng. "Active storage framework for object-based storage device." 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06). Vol. 2. IEEE, 2006.
6. Zhang, Yu, and Dan Feng. "An active storage system for high performance computing." 22nd International Conference on Advanced Information Networking and Applications (aina 2008). IEEE, 2008.
7. John, Tina Miriam, AnuradharthiThiruvenkataRamani, and John A. Chandy. "Active storage using object-based devices." 2008 IEEE International Conference on Cluster Computing. IEEE, 2008.
8. Devulapalli, Ananth, et al. "Design of an intelligent object-based storage device." Ohio Supercomputer Center, Tech. Rep.[Online]. Available: http://www. osc. edu/research/network file/projects/object/papers/istor-tr. pdf (2009).
9. Son, Seung Woo, et al. "Enabling active storage on parallel I/O software stacks." 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST). IEEE, 2010.
10. Xie, Yulai, et al. "Design and evaluation of oasis: An active storage framework based on t10 osd standard." 2011 IEEE 27th Symposium on Mass Storage Systems and Technologies (MSST). IEEE, 2011.
11. Nirmala, S. Jaya, S. Mary SairaBhanu, and AhteshamAkhtar Patel. "A comparative study of the secret sharing algorithms for secure data in the cloud." International Journal on Cloud Computing: Services and Architecture (IJCCSA) 2.4 (2012): 63-71.
12. Perlman, Radia. "File system design with assured delete." Third IEEE International Security in Storage Workshop (SISW'05). IEEE, 2005.
13. Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." 2010 proceedings ieeeinfocom. Ieee, 2010.