ISSN No:-2456-2165

Enhancing Security Supervision for DifferentTypes of Data and Endow Different Security Techniques

Shrihari M R. (Assistant Professor), Shamanth R., S L S Aditya Reddy, Sanjay Kumar S., Tejas S K
Department of Computer Science andEngineering
S J C Institute of Technology, Chickballapur

Abstract:- Lately, progressions in Internet and cloud innovations have prompted a critical expansion in Security issues and urge to learn implementation of better security methodologies. Thus, there is a demand for a platform to learn about intelligent techniques that can protect users from the cyber-attacks. Also, advancements of new technologies led to use of trending authentication techniques. Due to inefficient security techniques and due to less knowledge, there is an gradual increase in the number of victims. Generally, when it comes to learning or demonstration of how a security is provided to a content, it is disclosed or non-understandable. Thus, to overcome most of such problems we develop a software or an interface where an individual can systemize divergent type of data and endow different security techniques.

Keywords:- *Encryption, Decryption, Public Key, Private Key, Key Generation and Exchange ,Hadoop.*

I. INTRODUCTION

As we live in a modern world where internet is used in every single field and in every kind of technological applications, it raises to issues in authentication, authorization, safety, privacy security and a lot more. In today’s world, we as users focus on trending methods of authentication techniques such as fingerprints, pattern matching, image password etc.

Currently there are a variety of authentication techniquesbut major of the approaches are application-based approaches which again tend to lower the security of a provided security file. We develop an interface which is a file-based approach that helps us to study and observe the security techniques for different types of data. Our main objectives of this project are to Study the security

Techniques and implement the secured proposed system, Storing the data with privacy preservation in storage system, Secure data, prevent it from breaches and provides security against unauthorized access or intrusions, implementing an interface which showcase organizing data based on extension and distinctsecurity methods applied for individual type of data Generally we use algorithms such as Chacha20- poly1305, Argon2id and X25519. supposed to impart it to the next party. we use it for keyexchange in our project.

The libsodium library is used for all cryptographic algorithms.

- **CHACHA20-POLY1305:** Just as the AES algorithm, Chacha20-poly1305 is a symmetrical block cipher algorithm. The key-size ofChaCha20 is either 128 or 256 bits. ChaCha20 is a 256-bit stream cipher for symmetric encryption. ChaCha20-Poly1305 is an Authenticated secured encryption with extra data calculation, that consolidates the ChaCha20 stream figure with the Poly1305 message confirmation code. Its utilization in IETF conventions is normalized in RFC 8439.It has quick programming execution, and without equipment speed increase, It is quite quicker than AES-GCM. In our project, we will be using this algorithm for symmetric encryption.

  It’s designed to have both high performance and high security. It can be implemented efficiently in pure software. By avoiding secret-dependent memory accesses and conditional branches in its construction,it’s immune to many forms of timing side-channel attacks that software implementations of other algorithms. The best result on ChaCha is a key recovery attack on its 7-round version, with 2237.7- time complexity (the exact unit is unclear) using output data from 296 instances of ChaCha.
- **ARGON2ID:** In our project we use Argon2id for password-based key derivation. Argon2d expands protection from GPU breaking assaults. It gets to the memory cluster in a secret phrase subordinate request, which decreases the chance of time-memory compromise (TMTO) assaults yet presents conceivable side- channel assaults. Argon2i is advanced to oppose side-channel assaults. It gets to the memory exhibit in a secret phrase free request.
- **X25519:** X25519 is a Diffie-Hellman calculation utilized for key understanding. Each run of a convention ought to utilize new boundaries chose indiscriminately. The boundaries for each run is called a ephemeral orbrief key. Since each run of the convention should utilize new boundaries it isn't helpful to recover a private key produced aimlessly. The public key is more straightforward to separate since you are.
- **HADOOP:** Hadoop was a significant improvement in the large data region. Truth be told, it is suggested as the reason for present day cloud data capacity. Hadoop leftist's PC power and makes it workable for organizations to break down and inquiry huge data sets in a quantifiable mannerutilizing free, open-source programming and cheap, off-the-rack program. This was a huge advancement since itgave an option in contrast to restrictive data warehouse (DW) arrangements and shut data designs that had overwhelmed the day up to that point. With the presentation of Hadoop, associations were soon ready to access and store a lot of data, developing processing

power, mistake resistance, data the executive's adaptability, lower costs contrasted with DWs, and more noteworthy heartiness - simply continue to add more elements. At long last, Hadoop made ready for future improvements in data examination, for example, the sendoff of Apache Spark

II. LITERATURE

In this relevant paper [1], creators Consider the qualities of huge information and the prerequisites of information security oversight, expand the broadly utilized provenance model PROV-DM algorithm system by subtyping and adding new connection definition, and propose a major information provenance model BDPM for information management. BDPM model backings the provenance portrayal of different information types and various information handling modes to address the whole information change process through various partsin the large information framework and characterizes new relations to improve provenance investigation capacities.

Proposes a mystery sharing gathering key administration convention (SSGK) to safeguard the correspondence interaction and shared information from unapprovedaccess. Not quite the same as the earlier works, a gathering key is utilized to scramble the common information and a mystery sharing plan is utilized to convey the gathering key in SSGK. The broad security and execution investigations demonstrate that our convention exceptionally limits the security and protection dangers of sharing information in distributed storage and recoveries around 12% of extra room.[2]

Investigated the gamble of safety and protection spillage in the assortment, transmission, capacity, use and sharing of clinical large information, and laid out a clinical huge information security and security spillage risk marker framework, in the existence pattern of clinical enormous information, the two phases of information stockpiling, information use and sharing might create more unmistakable issues of information security and security divulgence, while the information assortment and information transmission are somewhat less.[3]

The paper [4] center has been given to get medical services private information in the cloud utilizing a haze processing office. To this end, a tri-party one- round verified key understanding convention hasbeen proposed in view of the bilinear matching cryptography that can produce a meeting key among the members and impart among them safely. At last, the private medical care information are gotten to and put away safely by carrying out a decoy method.[4]

In this pertinent paper [5], Authors proposes an incorporated philosophy to characterize and get enormous information prior to executing information versatility, duplication, and investigation. The need of getting enormous information not entirely settled by grouping the information as indicated by thegamble sway level of their items into two classifications: private and public.[5]

Complete audit of the literary works on information security and protection issues, information encryption innovation, and relevant countermeasures in distributed storage framework. In particular, initial an outline of distributed storage, including definition, grouping, design and applications. Furthermore, itemized examination on difficulties and necessities of information security and security insurance in distributed storage framework.[6]

Comparison of AES 128,92 And 256-Bit Algorithmfor Encryption and Description File. Compares encrypted and decrypted file test time produced results and CPU usage for both the processes everything measured in seconds.[7]

Here it Proposes a 32-bit AES implementation on Xilinx Spartan-3 using 148 slices, 11 BRAMs and achieving 647 Mbps at 278MHz.[8]

The plan of computerized mark and encryption administrations from the early improvement of the e-learning framework could give a smooth change of framework handiness and clients acknowledgment to ensure secrecy, non-disavowal, and confirmation. Execution of advanced mark and encryption procedures.[9]

Proposes an ordering plan to encode the first table's tuples into bit vectors (BVs) before the encryption. The subsequent file is then used to limit the scope of recovered encoded records from the cloud to a little arrangement of records that are possibility for the client'squestion. In view of the ordering plan, we then, at that point, plan a framework to execute SQL questions over the encoded information. The information are scrambled by a solitary randomized encryption calculation, to be specific the Advanced Encryption Standard-Cipher- Block Chaining (AES-CBC). In the proposed conspire, we store the file values (BVs) next to user, and we stretch out the framework to help a large portion of social polynomial math administrators, for example, select, join, and so forth. [10]

III. PROBLEM DEFINITION

Nowadays internet users are gradually increasing, so cyber security plays an important and major role in restricting the entry of unauthorized users. Users aren't aware of the privacy breach and doesn't have any idea regarding supervision encryption and decryption techniques.

Data in files will be very important for the users, it may contain personal, professional, and other information that is confidential, sensitive. So, we have identified thisas a problem for which a solution can be implemented and designed accordingly.

File security is about protecting your business important information in the eyes of the test by using strict access control measures and seamless clearance. In addition toenabling and monitoring security access controls, deleting data storage also plays an important role in protecting files. Always optimize file storage by deleting old, old, and unwanted files to focus on important business files. Deal with data security threats and storage malfunctions with periodic updates and enhancements to your file protection strategy.

IV. PROPOSED WORK

In this project we are providing two types of security techniques, the first one concerned with alphanumerical password and second one is built using Diffie Hellman key exchange protocol. These two are proposed using AES-128-bit algorithm to provide greater security and mainly focuses on the password given by authorized users.

Most individuals struggle to create and remember passwords, resulting in weak passwords and password reuse. Password-based encryption is substantially less safe because of these improper practices. That's why it is recommended to use the built-in password generator and use a password manager like Bit warden, where you are able to storethe safe password.

V. METHODOLOGY AND IMPLEMENTION

It uses authenticated encryption. The sender must provide their private key, a new shared key will be computed from both keys to encrypt the file. Recipient must provide their private key when decrypting also. this way can verify that the encrypted file was not tampered with and was sent from the real sender. Using public key encryption instead of a password:If you are encrypting a file thatyou are going to share it with someone else, then youprobably should encrypt it with the recipient public key and your private key.

A. Sharing Encrypted Files:

If you plan on sending someone an encrypted file, it is recommended to use your private key and their public key to encrypt the file. The file can be shared in any safe file sharing app.

B. Sharing the public key:

Public keys are allowed to be shared, they can be sent as public file or as text. Never share your private key to anyone! Only publickeys should be exchanged.

C. Storing the Public & Private keys:

Make sure to store your encryption keys in a safe place and make a backup to an external storage. Storing your private key in cloud storage is not recommended.

D. Sharing Decryption Passwords:

Sharing decryption password can be done using a safe end-to-end encrypted messaging app. It's recommended to use a Disappearing Messages feature, and to delete the password after the recipient has decrypted the file.

Never choose the same password for different files.

To make use of this web application, the user must provide a valid file and a password in the upload column where the data is checked and gets properly uploaded into storage space. The password gets hashed and a secure key is derived from it and provides the security /encrypted file.

Encryption and Decryption Algorithm pseudocode: Step1: import modules such as java util Base64, Crypto sub modules such as Cipher, Key Generator,

Secret Key, ChaCha20ParameterSpec,
SecretKeySpec;

- Step 2: Creating CHACHA20 encryption class.
- Step 3: Generate Key
- Step 4: Get Cipher Instance
- Step 5: Create ChaCha20ParameterSpec Step 6: Create SecretKeySpec
- Step 7: Initialize Cipher for ENCRYPT_MODE Step 8: Get Cipher Instance
- Step 9: Create ChaCha20ParameterSpec Step 10: Create SecretKeySpec
- Step 11: Initialize Cipher for DECRYPT_MODE Step 12: Perform Decryption
- Step 13: using the inverse process of encryption steps asits a symmetric model.

Final Step: Obtaining the original data provided by user Working of Chacha20-poly1305

The ChaCha20-Poly1305 algorithm as described in figure (fig a). Firstly, it takes an input a 256-bit key anda 96-bit nonce to encrypt a plaintext which will be provided by user, with a ciphertext expansion of 128-bit. In the ChaCha20-Poly1305 construction, ChaCha20 is used in counter mode to derive a key stream that is XOR operation with the plaintext. The ciphertext and theassociated data is then authenticated using a variant of Poly1305 that first encodes the two strings into one. Thus, the chacha20 keeps processing simultaneously with poly1305 for all the character keys that user provide. Thus, this combination algorithm makes key generation and encoding strings much easier and thus provides the encryption in the form of symbols for the user’s eyes. Since on viewing the encrypted file, all it appears are symbolic characters the attacker tends to be confused on the algorithm used thus our data gets enhanced security.

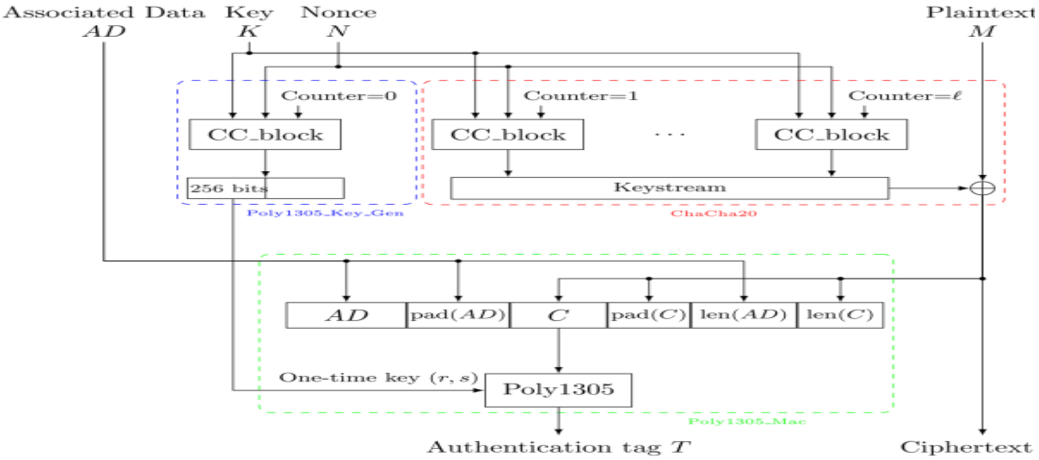

Fig. 1: working of chacha20-poly1305 algorithm

VI. RESULTS AND DISCUSSION

Functionalities that are available in the project are Secure encryption/decryption of files with passwords or keys, Secure random password generation, Asymmetric key pair generation, Authenticated key exchange, Password strength estimation.

The designed project website runs locally in any browser (recommended chrome/edge/firefox).

Here the process to do is quite simple and easy for users. So here, the project is a website hence the user have to run it in the browser. The execution consumes less time.

Firstly the user is directed to login page where he/she must register themselves and login. Oncelogged in User can select the type of file they want to encrypt. As done, user can see the option in between encryption and decryption.

On encryption, users have two kinds of methods. One is password and the other is public key method. Once choice is made, the encoded (.en) file can bedownloaded through Hadoop application. [cloud storage can be used for future enhancement].

On Decryption, user have to upload the .en file which is encrypted along with the same password used for encryption. Thus, we can retrieve the readable file.

Finally, the main discussion is about the security level of password that is used for encryption, since chacha20-poly1305 is used the security level is quitebetter than AES in terms of speed and performance as its totally independent of hardware And also project provides security to different types of files (PDF,DOC,CSV,IMG,MP4) endowing differentmethods(Password or diffie-hellman key exchange).

Medical data:

SL NO	AGE	BMI
1	19	27.9
2	18	33.77
3	28	33
4	33	22.705
5	32	22.88
6	31	25.74
7	46	33.44
8	37	27.74
9	37	29.83
10	60	25.84

Table 1

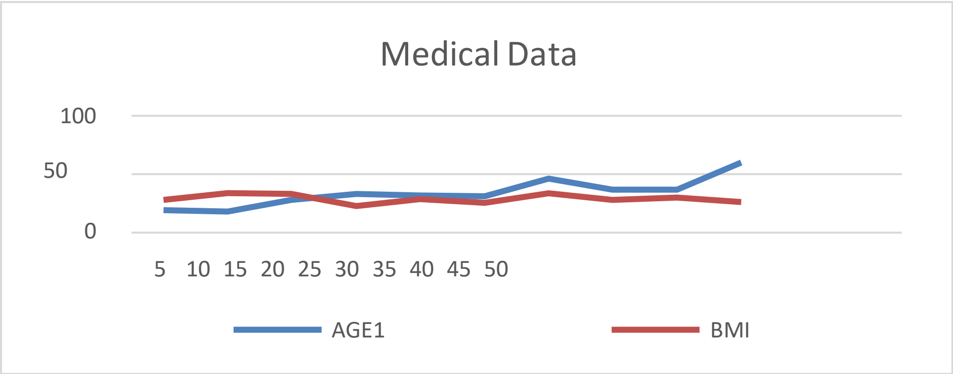

Fig. 2

VII. CONCLUSION

The final output is a web interface model which mainly focuses on securing the datasets or the different types offiles. The webpage model developed is simple to be navigated and efficiently accessed. Endowed security methods processing effectively and efficiently for different types of file loaded. The encrypted file can be easily accessed and retrieved by the user. Later retrieving the original file that was encoded by using theencoded file and the password.

REFERENCES

[1.] Yuanzhao Gao, Xinguyan Chen and Xuehui Du, “ABig Data Provenance Model for Data Security Supervision Based on PROV-DM Model”, 2020, National Key Research and Development, China 2018YFB0803603.DOI:10.1109/ACCESS.2020.2975820. (Journal)

[2.] Si Han, Ke Han and Shouyi Zhang, “A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era”, 2019, School Youth Fund Project of the China University 10818435. DOI: 0.1109/ACCESS.2019.2914862. (Journal)

[3.] Rong Jiang, Mingyue Shi and Wei Zhou, “A Privacy Security Risk Analysis Method for MedicalBig Data in Urban Computing”, 2019, Yunnan University of Finance and Economics, DOI:10.1109/ACCESS.2019.2943547(Journal)

[4.] Hadeal Abdullaziz, Sk Rahman, Shamim Hossain and Atif Alamri, “A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing- Based Cryptography”, 2017, College of Computer and Information Sciences, King Saud University, DOI: 10.1109/ACCESS.2017.2757844. (Journal)

[5.] Ismail Hababeh, Ammar Gharaibeh, Samer Nofal and Issa Khalil, “An Integrated Methodology forBig Data Classification and Security for Improving Cloud Systems Data Mobility”, 2018, Qatar Computing Center, DOI: 10.1109/ACCESS.2018.2890099. (Journal)

[6.] Pan Yang, Neal Xiong and Jingli Ren, “Data Security and Privacy Protection for Cloud Storage: A Survey”, Henan Academy of Big Data/School of Mathematics andStatistics, DOI: 10.1109/ACCESS.2020.DOI. (Journal)

[7.] Ria Andriani, Stevi Ema Wijayanti and Ferry Wahyo Wibowo, “Comparision Of AES 128, 192 And 256 Bit Algorithm For Encryption And Description File”, 2018, 3rd International Conference on Information Technology, Yogyakarta, Indonesia. (Conference)

[8.] Chi Wu Huang, Chi Jeng Chang, Mao Yuan Lin and Hung Yun Tai, “The FPGA Implementation of 128-bits AES Algorithm Based on Four 32-bits Parallel Operation”, Department of Industrial Education National Taiwan Normal University. (Conference)

[9.] ISMAIL HABABEH (Member, IEEE), AMMAR GHARAIBEH (Member, IEEE), SAMER NOFAL (Member, IEEE), AND ISSA KHALIL,“An Integrated Methodology for Big Data Classification and Security for Improving Cloud Systems Data Mobility”, School of Electrical Engineering and Information Technology, German Jordanian University. Vol 9,2019.

[10.] Ahmad Baihaqi and Obrina Candra briliyant “Implementation of RSA 2048-bit and AES 128-bit for Secure E-Learning Web-based Application.” National Crypto Institute Bogor, Indonesia. (Conference).

[11.] Huiyu Zhou “Privacy-Aware Secure Anonymous Communication Protocol in CPSS Cloud Computing” School of Information Science and Engineering, Qufu Normal University, Rizhao 276826, China School of Cyber Science and Engineering, Shandong University of Political Science and Law, Jinan 250014, ChinaSchool of Informatics, University of Leicester, Leicester LE1 7RH, U.K.

[12.] Hao Yan “Efficient Identity-Based Public Integrity Auditing of Shared Data in Cloud Storage With User Privacy Preserving” School of Network Security, Jinling Institute of Technology, Jiangsu 211169, China Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Jiangsu 210003, China

[13.] Lidong Han “An Efficient and Secure Public Key Authenticated Encryption With Keyword Search in the Logarithmic Time” Key Laboratory of Cryptography Technology of Zhejiang Province, Hangzhou 311121, China school of Information Science and Technology, Hangzhou Normal University, Hangzhou, Zhejiang311121, China School of Computer Science and Technology, Qingdao University, Qingdao 266071, China

[14.] MOHAMMED BINJUBEIR 1, ABDULGHANI ALI AHMED , “Comprehensive Survey on Big data Protection” Centre of excellence in Information assurance, King Saud University, Saudi Arabia.

[15.] ANA KOVA.EVI. 1, NENAD PUTNIK1, AND OLIVER TO. KOVI. “Factors Related to Cyber Security Behaviour” Faculty of Security Studies, University of Belgrade, 11000 Serbia. Laboratory for experimental psychology, University of Belgrade, 11000 Belgrade Serbia.