JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Securing Internet of Things (IoT) Devices : AES vs Simon-Speck Encryptions in Comparative Method

[1] Sonam Rajput, [2]Dr. Arvind Kaurav, [3]Prof. Nehul Mathur
[1]M.tech Student , [2]Professor, [3]Assistant Professor
[1,2,3]Department of Electronics and Communication (EC)
[1,2,3] Bhopal Institute of Technology, Bhopal (M.P.) INDIA,

Abstract : This paper present Internet based secure data transmission is an emerging area of research, where most of the data transfer infrastructure is moving to make their service and delivery more efficient. In this Dissertation our work approach lead behind the secure data transmission data get upload over the data server and its different user due to different ownership. The concept behind the research is taken a secure and reliable algorithm, approach which can find the solution for data security redundancy optimization over the data store. The proposed method discussed about the file level distribution and redundancy detection using file level chunking, where as to transmit and store the data AES (Asymmetric encryption system) algorithm is used to provide data security. For improvement of the hash calculation use SHA – 512, with the help of SHA -2 obtain secure file detection faster as compare to other methods. The proposed research work shows better result as compare to other previous encryption methods in terms of block size, word size, hash output, rounds and time complexity**.**

Keywords— Asymmetric Encryption System (AES), Simple Hash Algorithms (SHA),National Security Agency (NSA), Secure Data Transmission, MD-5, block size, word size, hash output , number of round and Finite Field Construction.

I. INTRODUCTION

Encryption is based on cryptography. Cryptography is the art of hiding information to make it unreadable without special knowledge or a key. The earliest recorded examples include the use of non-standard hieroglyphs as a substitute for the hidden information, and the use of personal identification marks such as seals, emblems, or logos for authentication. The receiver of the sealed item would have a copy of the true mark to use to authenticate the one presented.

Encryption allows a person to hide the meaning of information or messages in such a way that only those who know the secret method may read them. For a very long time, people have had many different reasons for wanting to hide information from others. The earliest historic examples were for hiding trade secrets, military secrets, and secret correspondences between spies and lovers. These same encryption principles are now used to safeguard your internet communications.

A. Advanced Encryption Standard (Aes)

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cyber security and electronic data protection.

The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or non-commercial programs that provide encryption services. However,

Nongovernmental organizations choosing to use AES are subject to limitations created by U.S. export control.

II. LITERATURE SURVEY

The literature survey discusses some very new techniques carried out by many researchers related to the field of Securing Internet of Things (IoT) Devices. There are many methods introduced of AES vs Simon-Speck Encryptions in Comparative Method.

Ananya B L, et.al. (22 March 2023) - Nowadays data sharing over the internet is a major and critical issue due to security problems. So more security mechanisms are required to protect the data while sharing through an unsecured channel. we present one such algorithm for data confidentiality while sharing. Advanced Encryption Algorithm (AES) is a symmetric encryption algorithm that provides more encryption security than its predecessor Data Encryption Standard (DES). In this review paper, we compare the various applications, advantages, and shortcomings of this complex algorithm by also comparing them to other standard algorithms [01].

Rahul Neve et.al. (16 July 2023) - The lightweight cryptographic (LWC) algorithm is used for resource constraint devices. The performance analysis and development of LWC is for achieving better data security in resource constrained mobile devices for effective implementation. Literature survey on LWC was carried out where it was observed that the implementation of two well-known algorithms "SIMON" and "SPECK" are in latest research as per future technological requirements. On comparing SIMON & SPECK algorithms with conventional blocks, lightweight block ciphers the following challenges that are required to be mitigated by including usage of minimal hardware overhead in proposed design (e.g., time, memory consumption), viz. use of low-cost smart mobile devices, with minimal power, low energy consumption and improved security performance. Algorithms were implemented on the Raspberry Pi 3 with 1GB RAM, Quad Core 1.2GHz Broadcom BCM2837, with 32-bit Raspbian Operating System of 5V and current of 2 mA. Input to the algorithm is fed as text with varying size viz. 100kB, 200kB, 300kB, 400kB, 500kB.An attempt is made to developed hybrid LWC algorithm by using key scheduling logic of SPECK and Round function logic of SIMON. Experiment was performed using text file as inputs with varying sizes. On comparing the actual SIMON algorithm with HybridSIMON_SPECKey algorithm it is observed that encryption and decryption time comsuption is 50% less. Thereby an improvement is observed in time and energy efficiency. Similarly in case of memory consumption of SPECK Algo with Hybrid SIMON-SPECKey algorithm it consumes an average 19% less memory during encryption as well as decryption [02].

Baiq Yuniar Yustiarini et.al. (07 September 2022) - Delivering information from Internet of Things (IoT) devices to a cloud server possesses several security issues, e.g. information eavesdropping, modification, and theft. Therefore, communication between IoT devices and the cloud server should be protected by encryption methods. However, there are few encryption techniques options that are suitable for the need for lightweight communication as demanded by the IoT devices. Due to these circumstances, the NSA launched an encryption algorithm for IoT named Simon and Speck, which are maximally efficient while still providing the advertised level of security, as determined by the key size. This study aims to test and compare the Simon-Speck and AES encryption algorithms and their effect on networking performance on IoT devices. The parameters in this test are delay, throughput, the efficiency of memory usage from the encryption algorithm, and the value of the avalanche effect. Experimental results show that the Speck algorithm outperforms the Simon and the AES algorithms in terms of communication delay and memory usage. Regarding the avalanche effect values, the Simon algorithm possesses the highest avalanche effect value on average against the Speck and the AES algorithms [03].

L.Mary Shamala et.al. (2021) - Internet of Things is a worldwide set-up of interconnected entities that permits millions of devices to communicate with each other. Combined with reliable communication, ensuring security concerning confidentiality, integrity, and authenticity is a great challenge in IoT. Unsecured IoT devices open gateway for attacks. Unprotected and vulnerable devices, at times, allow easy entry for hackers, enabling them to have access to the shared network and personal, corporate assets. Conventional security measures are not suitable and cannot be applied to IoT technologies because of their minimum storage, low processing capacity, and limited computing power. Besides, scalability and heterogeneity issues arise when a variety of devices are interconnected. This paper presents the security threats and requirements of IoT cryptography, technology, and trends. The paper also discusses the challenges faced and the comparison of solutions already existing in IoT security [04].

Pejman Panahi et.al. (13 January 2021) - All smartphones, notebooks, or other communication devices could connect to the cloud, so the data are accessible everywhere. When these devices are interconnected through the internet, they make an Internet of Things (IoT) network that exchanges data among network nodes and other services. IoT has a broad application area from smart applications to various industrial usages. However, the high volume of data transferred in the IoT network makes it crucial to implement mechanisms to transfer the data safe and secure. Enciphering is one of the best techniques to ofer end-to-end security. Considering an IoT network, nodes have restricted resources, and applying classical cryptography methods are costly and not efcient, so lightweight block ciphers are one of the sophisticated solutions to overcome security drawbacks in this scope. In this paper, ten lightweight algorithms involve AES, PRESENT, LBlock, Skipjack, SIMON, XTEA, PRINCE, Piccolo, HIGHT, RECTANGLE tested to evaluate their performance for key factors such as memory usage (RAM and ROM), energy consumption, throughput, and execution time for both encryption and decryption modes over cloud transmission. We have done simulations using Raspberry Pi 3 and Arduino Mega 2560 as the leading devices in the IoT scope. As a result, this paper will help IoT developers to choose the right platform and enciphering algorithm to set up a secure network due to multiple factors like energy and memory usage, especially for software platforms [05].

Abdulrazzaq H. A. Al-Ahdal et.al. (31 Oct 2020) - Modern applications consist of different types of control devices and sensors that connect to the Internet. These applications are new approved technologies called the Internet of Things. Nowadays, these new technologies have gained a great interest in the field of research because of their existence in several diverse fields and due to the rapid development of these technologies. Communication between these devices generates a large amount of private and sensitive information and data between them. Therefore, maintaining the confidentiality of that data and information in the Internet of Things is of great importance. Mathematical cost (complex mathematical operations) and the number of cycles in traditional cryptographic algorithms leads to a large use of memory and energy waste for devices with limited resources, which makes traditional cipher algorithms inappropriate for Internet of Things devices. A fast and LW algorithm called NLBSIT has been proposed in this regard, which provides the requisite protection and resource constrained confidentiality of data on IoT devices [06].

Li Ning et.al. (2020) - The most serious challenges currently faced by healthcare environment is the decision making related to the installation of the most suitable and appropriate lightweight authentication cipher that could provide solutions towards the authentication issues prevailing in IoHT devices. This decision making becomes more troublesome and tricky due to the number of factors that are taken into account such as availability of many existing ciphers, complex and multiple numbers of requirements involved and frequent changing of these requirements from one platform to another. This decision making is also hampered by the nature of IoT devices operating in healthcare environment as they come up with limited functionality, processing, bandwidth and memory. In this regard, we present an evaluation framework focuses upon the selection of best light weight cryptographic ciphers by considering the most important parameters or requirements of criteria. The proposed framework considers the requirements like performance, physical and security as suggested by widely accepted standards such as National Institute of Standards and Technology (NIST) and International Standard Organization standard such as ISO/IEC 29192 for building evaluation criteria. This framework evaluates and selects the best lightweight cryptographic among the 10 ciphers i.e. PRESENT-80, Scalable Encryption Algorithm (SEA), HIGHT, Lightweight Encryption Algorithm (LEA) Advanced Encryption Standard (AES-128), mCrypton, NOEKEON, Klein, Camellia and Tiny Encryption Algorithm (TEA) for the purpose of evaluation in IoHT environment [07].

Chandel, et.al. (2019, December) - The present study Nowadays, using of internet is increasing. Everyone is more active on the social networking sites and data exchange has been increased rapidly. Here, data security plays a vital role. Encryption and decryption algorithms are used to escape the data from any third party attacks. There are use various type of cryptographic algorithms to encrypt data. AES algorithm is more widely used as a symmetric encryption algorithm and it is easy to use and robust. AES is the most powerful cryptographic algorithm which is used in most of the applications which we use in our daily lives like messenger etc. AES cryptography packages are available almost on every platform such as Turbo C++, DEV C++ etc.There are encrypt and decrypt the data using different combinations from the malicious attack. This algorithm give different key sizes for encryption 10, 11 and 14 rounds which are used for 128-bit, 192-bit key and 256-bits block cipher respectively. In RSA it is an asymmetric type of cryptography i.e. there are 2 keys used open key and private key and we are using the product of any 2 large prime number for the purpose of security. RSA is more thread safe. On the other hand Advanced Encryption Standard is a single key type of cryptography. AES involves only a single key for encryption and decryption process [08].

Hafsa, et.al. (2019, March) - This paper reviews suggested a novel hybrid cryptosystem that uses advantages of both symmetric key and asymmetric cryptographic ways. The main of the proposed architecture is a modular multiplication unit, which extends operations realized for an optimized ECC cryptosystem in order to support the Mix Columns operation of an optimized AES algorithm. There are evaluated our system design on DE2-115 board. Findings proved that our proposed method demands less execution time, less area occupation and less total power dissipation compared with others methods. As a continuity to this work, we propose to design an optimized Elliptic Curve Digital Signature (ECDSA) cryptosystem which can be implemented in one ARM based on MP core SoC such as with Zynq FPGA. This prototype will be applied in several input conditions like images and video signals. To prove the security of the proposed system, hardware countermeasures against Side-Channel Attacks (SCA) will be studied and proposed [09].

Ghosh, et.al. (2019, December) - Several approaches of secured message transactions on cloud data are studied and analyzed. A secured cloud data message transaction protocol with variable length key has been designed, developed and applied through the use of Advanced Encryption Standard (AES) using the Python programming language. The length of the used key is given as input by the user followed by the selection of a secret key which is fed into the AES cryptographic system with the desired cloud data message thus producing the Cipher text that is to be transmitted to the destination. In the receiver end, the reverse process is performed with the same key on the received Cipher text and the plaintext is retrieved. A comparative study with the two existing approaches has been performed and presented. The presented security mechanism can be applied on any secured cloud data message transactions that may be either in financial or in e-commerce based cloud environment [10].

Sönmez, et.al. (2019, September) - Two important features have been selected for this attack. Which of these features is better can be understood by looking at the auc (area under curve) values in the Table II. Among the applied models, XGBoost and Random forest have the highest auc values. These models considered the” cycle on average” feature more important. Since the” deviation of cycle” feature was more important than the GBM and Decision Tree models, the auc value was slightly lower. When these results are compared, it is seen that the” cycle on average” feature is a more significant side channel leakage for time-driven cache attacks [11].

Bhattacharjya, et.al. (2019) - So at the beginning of discussing the major contributions of the work, lets discuss the encryption level contribution, the SHRSA messaging scheme's 9 layered cipher's encryption with 1024 Bit RSA modulus, is shielding us from some of the scientic problems of RSA like, the very high computationally costly exponentiation modulo N problem, the exploitation of multiplicative property, low modular complexity with effortlessness, difficulty of the integer factorization problem of RSA, the exploitation of homomorphism property and speediness problem. There all know that all available RSA variants' encryption are able to solve two or three major problems of RSA but the SHRSA messaging scheme's encryption is resolving many problems of RSA as discussed in section III and section IV in details. Also the SHRSA messaging scheme's 9 layered cipher's encryption has proper protection from CCA and Short Plain- text Attack etc, along with protection to Snifng attack and the real- time Key negotiation issue also. Brute force attack is shielded by randomly changing the keys in synchronous time slot with 1024 Bit value [12].

Shvartsman, et.al. (2019, October) - A masking scheme for AES is presented which uses finite field construction variation with random masking to prevent higher-order power analysis. Field constructions are chosen to remove the co-variance between share leakage. Security analysis shows that this provides a high level of security against higher-order power analysis attacks. Although, the scheme requires inserting constant binary mapping matrices and a larger MixbColumns, the number of required registers is greatly reduced. As a result, 12% few logic gates are needed compared to the previous best design [13].

Iavich, et.al. (2018, October) - This paper reviews is described and analyzed two types of systems: Symmetric and Asymmetric cryptosystems. The paper provides new model of hybrid algorithm using AES and ElGamal cryptosystems. Special software tool was created and implemented for proposed system. Compared with encryption and decryption speed experimental research shows, that symmetric algorithm AES is faster, but asymmetric algorithm ElGamal is better to provide security. The symmetric algorithm AES requires very low computational power. AES is one of the best algorithms of symmetric encryption cryptography. ElGamal algorithm gives high throughput as compared to AES and other algorithms. The hybrid of AES and ElGamal algorithm has characteristics of both the algorithms. This makes the algorithm strong against vulnerabilities. This hybrid structure of AES and ElGamal provides more security by increasing the complexity. As the result shows, proposed AES & ElGamal hybrid algorithm model is comparatively better than ElGamal in terms of encryption / decryption time and better than AES in terms of its security. The complexity of the system is provided by combination of two algorithms. Given results can be implemented in aviation for flight control systems as well as other critical aviation information systems security ensuring [14].

III. PROBLEM FORMULATION

As per the literature survey is performed with different techniques and different result from the algorithms were monitored such as Content based , Chunking based, Hash Based and other different technique for data processing , security approach over data store . The techniques for security over the cloud data is also performed by different services to make it more secure and accessible.

Cryptographic technologies for data integrity and availability, based on Hash functions and signature schemes cannot work on the outsourced data.

Upon verifying different scenario and the available technique different short comes with the Existing algorithm.

AES-SHA2 with file based de-duplication which is taken as base for our research work. It is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users.

The following are the monitored points which identified as problem and further analyzed and performed further with enhancements.

1. Previous technique such as file based scheduling doesn't overcount all its data parts or internal division which can further be duplicate over the large amount of data . Thus an efficient monitoring is required which can further be monitor file duplicacy with data division.
2. AES algorithm takes an advantage of asymmetric encryption technique which is used by base paper, but still when talk about the multiple tenant, multiple ownership and multiple user over the data. Thus a security of key sharing is still a challenging issue which is faced by authors.
3. The Key length taken for the purpose of security in previous research is not considerable today. Today's scenario required an efficient and long length key for security purpose.
4. The existing approach for security uses MD5 for the hashing for content matching, but the MD5 algorithm faces collision issue with value generation. Hashing algorithm is the best practice to have long hash value.
5. A combination of MD5 and AES is taken for the consideration which is neighther more secure while talking about key exchange, again an extra procedure is required to do the key exchange. Thus it exhibit extra computational time as well as computation cost for cloud server.
6. A file level de-duplication algorithm by file hash MD5 is used, which can come under collision scenario and product false result when it terms to large number of server data files.
7. A consideration of Blowfish which is symmetric, as well as a fast security encryption algorithm can be taken, but still a large data file need more enhance & fast approach than blowfish.
8. Blowfish exhibit 4S block, having 128 value in each. This can be a focused area to work with and reduce on.
9. The existing algorithm take advantage over previous traditional techniques but still more refinements are required as per todays standard. Thus a better security, hashing mechanism can make it more reliable and executable to tackle with current security and cloud scenario in the world.

IV. PROPOSED MODAL

In the most of the previous work focus on data encryption few of them focus on data duplication avoiding and focus on secure data transmission. A balanced method, that's work on both point security as well as data security problems.

A. Problems to Overcome In This Proposed Work

In the previous work main focus on two problems first one is data privacy and second one is secure data integrity, these are the major two problems in this proposed work on these two problems**.**

Data Privacy

Unauthorized users who cannot prove ownership should not be able to decrypt cipher- text (encrypted) stored in the private storage.Additionally, the data server is no longer fully trusted in the system. Thus, unauthorized access from the data server to the plantext of the encrypted data in the data storage should be prevented. For the enhancement of data privacy and data security introduced a data encryption with hash value, which is check the data times to time as per the request of user. With the help of this phenomena user can check its data secure on data server or not. For the improvement of data privacy use advance AES based encryption system which generate higher level of data security

Data integrity

The secure data algorithm should guarantee tag consistency against any poison attacks. The secure data algorithm should allow the valid owners to verify that the data downloaded from the cloud storage have not been altered. For the improvement of data integrity also use the log in and log out time of users also manage data logs of file transfer and download by different users. Apart from the above two problems one more problem observe in the last decade that is secure data privacy. Now a day's many organizations suffer from secure data transmission problem that consume space and bandwidth and other resource of the system

Data Duplication

Data duplication is now a days emerging problem that is increase rapidly in the data servers. To avoid this problem is the main focus of the proposed work for avoiding this problem use hash algorithm. SHA–512 is hash and highly secure encryption algorithm use for data encryption. It generate a unique Hash value.

Proposed Method

The overall proposed method is divided into two sections. In the first section, upload the file on data servers and also check the duplicate file present or not in the data server. To avoid the duplication problem in the data server. In this case file is not uploading on the data server. After the verification of file, in the second stage upload file on data server with advance encryption system using AES.

V. SIMULATION AND RESULT

In this chapter simulate the proposed method and calculate the result based on different size file. For the simulation of the proposed method use Matrix laboratory software. Matrix laboratory is a well-known tool for such kind of algorithm implementation related to data hash encryption and hash value calculation. Matrix laboratory contain a rich function family of data encryption and decryption

Result Parameters and Simulation Tool

The result of proposed method for hash value based secure file transmission shown in this section, simulation of our proposed method and result calculation. In this proposed work with the help the Matrix laboratory versionR2015a (8.1.0.602) software and simulate whole proposed methodology in graphical user interface (GUI). The performance of the proposed algorithm is tested for different data file size that is shown in GUI windows. Basic configuration of our system is: Processor: Intel (R) Quad Core (VM) i5 – 3110 Central Processing unit @, 2.40 GHz with 4GB RAM: System type: 64-bit Operating System.

A. Encryption Time

This time is calculated by time taken to generate the output hash value.

$$H(t) = SHA(File)H(t) = SHA(File) \tag{5.1}$$

For small file size H(t) is low for higher size H(t) is high. There are different hash function available SHA – 1, MD5, SHA-2, SHA-256, SHA-384 and SHA 512.

B. Hash Value

Hash value is generated by hash function, different hash function SHA-2, SHA-256, SHA-384 and SHA 512 generate hexadecimal value. If the hexadecimal is large shows good result for example SHA512 generate 2^{512} different Hex codes it provide more secure hash value as compare to others.

C. Matrix LaboratoryGUI

A graphical user interface (GUI) is a graphical display that contains devices, or components, that enable a user to perform interactive tasks. To perform these tasks, the user of the GUI does not have to create a script or type commands at the command line. Often, the user does not have to know the details of the task at hand. The GUI components can be menus, toolbars, push buttons, radio buttons, list boxes, and sliders — just to name a few. In MATLAB, a GUI can also display data in tabular form or as plots, and can group related components

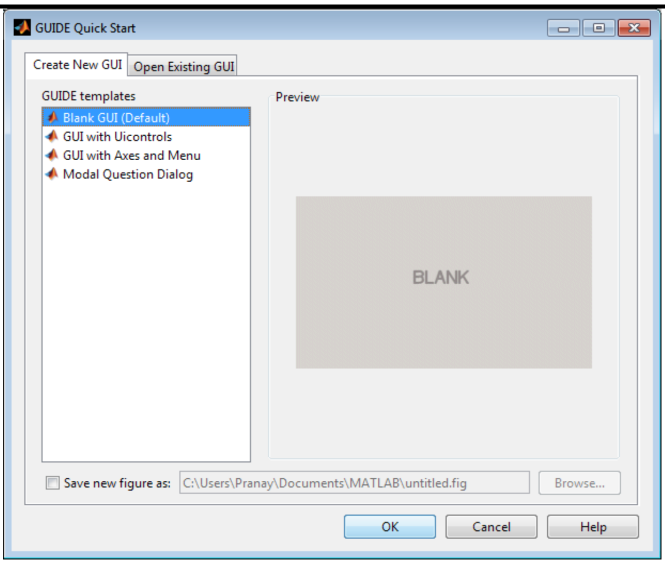


Figure 1: MATLAB basic GUI window

- Lay out controls of the GUI
- Wire up callbacks, the function that runs when you interact with the controls
- Gather data from the controls
- This series shows these basic skills. They allow you to make a wide array of GUIs very easily.

Steps of GUI –

Step – 1 for run the above project first start project for this run start1.m the proposed system. In this page in GUI that is shown in below figure 2.

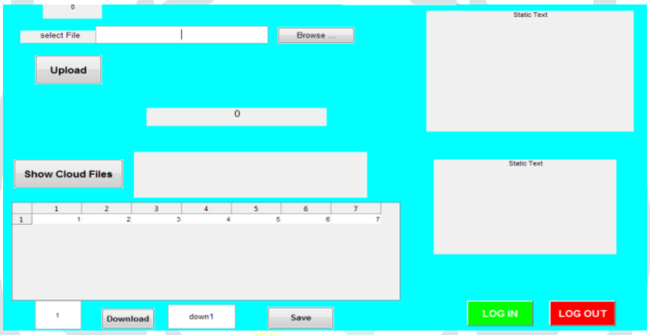


Fig. 2 Start point of the project

Step – 2. To start this page first click on Log in. When click on log in page a new window open in this window enter user name and id password. If id and passwords are correct then it start else shows the message of wrong id or password. In the below figure 3 shows the figure of log in window. There are two figures 3 shows the enter Id and password instruction.

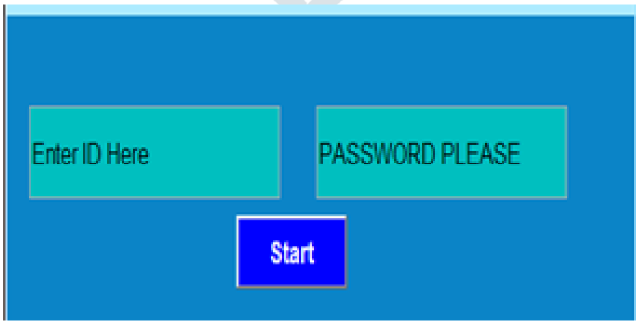
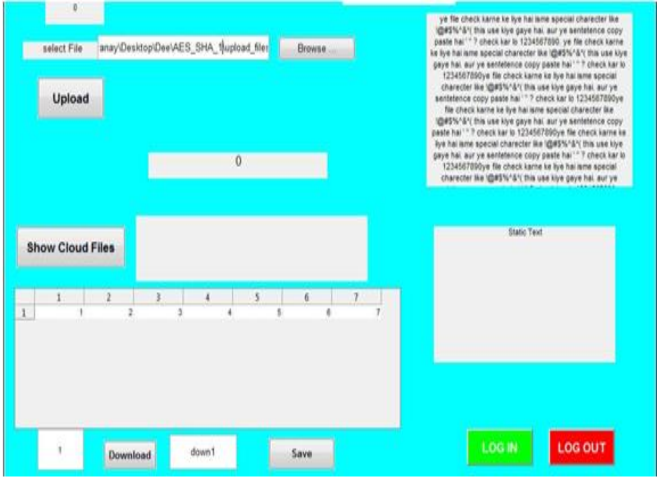


Fig. 3 ID and Password window

In the below figure 5.4 shows the users window for upload any file on data server. Just click on browse button and open a new window select your file at any location of your system. After that click on second push button that is **“Upload”** with the help of this calculate the hash values of the file.



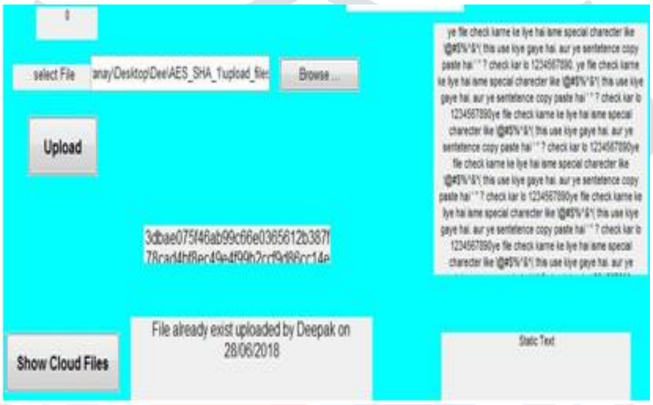
anay\Desktop\Dee\AES_SHA_1\upload_file

ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890. ye file check karne ke liye hai isme special charecter like !@#$%^&*( this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*( this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7

Fig. 4 (a) File Uploading Process First Selects the File

In the next step click on upload. When click on upload fist check this file is already exists or not if this file is already exist not upload on data server, otherwise upload encrypted hash value file.



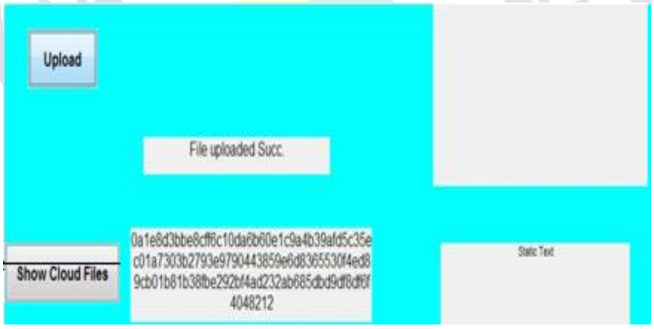
anay\Desktop\Dee\AES_SHA_1\upload_file

ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890. ye file check karne ke liye hai isme special charecter like !@#$%^&*( this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*( this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye sentetence copy paste hai`'" ? check kar lo 1234567890ye file check karne ke liye hai isme special charecter like !@#$%^&*(this use kiye gaye hai. aur ye

3dbae075f46ab99c66e0365612b387f
78cad4bf8ec49e4f99b2ccf9d86cc14e

File already exist uploaded by Deepak on 28/06/2018

Fig. 4 (b) Shows Calculated Unique Hash Value And Shows File Already Exists Not Upload On Cloud



File uploaded Succ.

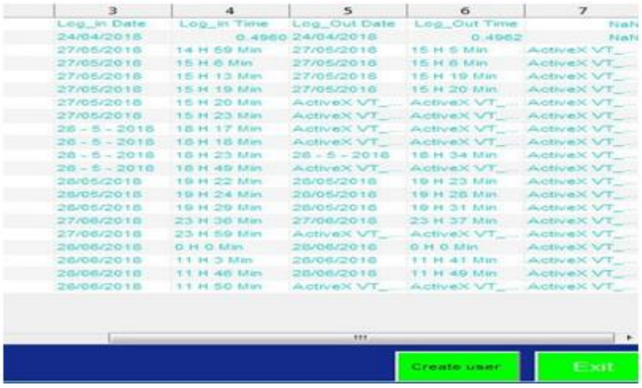
0a1e8d3bbe8cff6c10da6b60e1c9a4b39afd5c35e
c01a7303b2793e9790443859e6d8365530f4ed8
9cb01b81b38fbe292bf4ad232ab685dbd9df8df6f
4048212

Fig. 4 (c) Upload file – with unique hash Value and encrypted data

Step – 3 Data Server

In the below figure 5 shows the data server window of proposed work. Data server store all records of users and data verified. When user log in, user log out, date and time. In similar way admin have a Meta data of all files. In the proposed method for detecting users and its activity related to file upload for avoid secure data transmission problem. Use Meta data concept in which store the information of upload file such as date, time, user id, hash value and path of the file. Data server maintain two log tables first one is user log in table and second one is uploaded file Meta data table.

Step -4 Data Verifier



3	4	5	6	7
Log_in Date	Log_in Time	Log_Out Date	Log_Out Time	NaN
24/04/2018	0.4960	24/04/2018	0.4962	NaN
27/05/2018	14 H 59 Min	27/05/2018	15 H 5 Min	ActiveX VT_
27/05/2018	15 H 6 Min	27/05/2018	15 H 6 Min	ActiveX VT_
27/05/2018	15 H 13 Min	27/05/2018	15 H 19 Min	ActiveX VT_
27/05/2018	15 H 19 Min	27/05/2018	15 H 20 Min	ActiveX VT_
27/05/2018	15 H 20 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_
27/05/2018	15 H 23 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_
28 - 5 - 2018	18 H 17 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_
28 - 5 - 2018	18 H 18 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_
28 - 5 - 2018	18 H 23 Min	28 - 5 - 2018	18 H 34 Min	ActiveX VT_
28 - 5 - 2018	18 H 49 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_
28/05/2018	19 H 22 Min	28/05/2018	19 H 23 Min	ActiveX VT_
28/05/2018	19 H 24 Min	28/05/2018	19 H 28 Min	ActiveX VT_
28/05/2018	19 H 29 Min	28/05/2018	19 H 31 Min	ActiveX VT_
27/06/2018	23 H 36 Min	27/06/2018	23 H 37 Min	ActiveX VT_
27/06/2018	23 H 59 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_
28/06/2018	0 H 0 Min	28/06/2018	0 H 0 Min	ActiveX VT_
28/06/2018	11 H 3 Min	28/06/2018	11 H 41 Min	ActiveX VT_
28/06/2018	11 H 46 Min	28/06/2018	11 H 49 Min	ActiveX VT_
28/06/2018	11 H 50 Min	ActiveX VT_	ActiveX VT_	ActiveX VT_

Fig. 5 Shows Admin Window

VI. CONCLUSION

The conclusion of proposed method is mentioned here. Internet based secure data transmission is an emerging area of research, where most of the IT infrastructure is moving to make their service and delivery more efficient. In this Dissertation our work approach lead behind the secure data transmission data get upload over the data server and its different user due to different ownership. The concept behind the research is taken a secure and reliable algorithm, approach which can find the solution for data security redundancy optimization over the data store. The proposed method discussed about the file level distribution and redundancy detection using file level chunking, where as to transmit and store the data AES (Asymmetric encryption system) algorithm is used to provide data security. For improvement of the hash calculation use SHA – 512, with the help of SHA -2 obtain secure file detection faster as compare to other methods.

REFERENCES

[1] Ananya B L . Nikhitha V . S Arjun . Naveen Chandra Gowd "Survey of applications, advantages, and comparisons of AES encryption algorithm with other standards" Vol 2 , Issue 02, 22 March 2023.

[2] Rahul Neve, Dr. Rajesh Bansode, Vikas Kaul "Novel Lightweight Approach to Perform Cryptography for Data Security & Privacy in IoT Mobile Devices" ISSN:2147-67992147-16/July /2023.

[3] Baiq Yuniar Yustiarini; Favian Dewanta; Hilal Hudan Nuha "A Comparative Method for Securing Internet of Things (IoT) Devices: AES vs Simon-Speck Encryptions" 07 September 2022.

[4] L.Mary Shamala , Dr.G.Zayaraz , Dr.K.Vivekanandan, Dr.V.Vijayalakshmi "Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview" 2021.

[5] Pejman Panahi, Cüneyt Bayılmış, Unal Çavuşoğlu, Sezgin Kaçar "Performance Evaluation of Lightweight Encryption Algorithms for IoT Based Applications" 13 January 2021.

[6] Abdulrazzaq H. A. Al-Ahdal1, Galal A. AL-Rummana, G.N. Shinde, Nilesh K. Deshmukh "NLBSIT: A New Lightweight Block Cipher Design for Securing Data in IoT Devices" 31 Oct 2020.

[7] Li Ning , Yasir Ali , Hu Ke, Shah Nazir, And Zhao Huanli "A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things" 30, 2020.

[8] Chandel, Ankita, et al. "Comparative Analysis of AES & RSA Cryptographic Techniques."2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). IEEE, 2019.

[9] Hafsa, Amal, et al. "A New security Approach to Support the operations of ECC and AES Algorithms on FPGA."2019 19th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA). IEEE, 2019.

[10] Ghosh, Pronab, et al. "A Variable Length Key Based Cryptographic Approach on Cloud Data."2019 International Conference on Information Technology (ICIT). IEEE, 2019.

[11] Sönmez, Burcu, Ahmet Ali Sarıkaya, and Şerif Bahtiyar. "Machine Learning based Side Channel Selection for Time-Driven Cache Attacks on AES."2019 4th International Conference on Computer Science and Engineering (UBMK). IEEE, 2019.

[12] Bhattacharjya, Aniruddha, Xiaofeng Zhong, and Xing Li. "A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack."IEEE Access 7 (2019): 30487-30506.

[13] Shvartsman, Phillip, and Xinmiao Zhang. "Side Channel Attack Resistant AES Design Based on Finite Field Construction Variation." 2019 IEEE International Workshop on Signal Processing Systems (SiPS). IEEE, 2019.

[14] Iavich, Maksim, et al. "Hybrid encryption model of AES and ElGamal cryptosystems for flight control systems." 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC). IEEE, 2018.

[15] Kiruba, W. Mercy, and M. Vijayalakshmi. "Implementation and Analysis of Data Security in a Real Time IoT Based Healthcare Application." 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2018.

[16] Mekki, Neila, et al. "A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system." 2018 International Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, 2018.

[17] Rachmawanto, Eko Hari, et al. "Secured PVD Video Steganography Method based on AES and Linear Congruential Generator." 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). IEEE, 2018.

[18] Joshy, Amal, et al. "Text to image encryption technique using RGB substitution and AES." 2017 International Conference on Inventive Computing and Informatics (ICICI). IEEE, 2017.

[19] Adegbite, Oluwadara, and Syed Rafay Hasan. "A novel correlation power analysis attack on PIC based AES-128 without access to crypto device." 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS). IEEE, 2017.

[20] Balouch, Zaheer Abbas, Muhammad Imran Aslam, and Irfan Ahmed. "Energy efficient image encryption algorithm." 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT). IEEE, 2017.

[21] Anup Ashok Patil, Shital Mali, “Hybrid Cryptography Mechanism for securing self- Organized Wireless Networks”, IEEE, 2016.

[22] Raghav Mathur, Shruti Agarwal, Vishnu Sharma, “Solving Security Issues in Mobile Computing using Cryptography Techniques-A Survey”, IEEE, 2015.

[23] D. Zhang and H. Zhong, ”A text hiding method using multiple-base notational system with high embedding capacity,” Proc. of IEEE CISP, 2014

[24] Sánchez D, Batet M, Viejo A. “Automatic general-purpose sanitization of textual documents”. IEEE Trans Inform Forensics Secur 2013;8:853– 62.

[25] Martínez S, Sánchez D, Valls A. , “ A semantic framework to protect the privacy of electronic health records with non-numerical attributes,”. J Biomed Inform 2013;46:294– 303.

[26] B. Su, X. Ding, G. Liu and H. Zhang, ”An Information Hiding method for Text by Substituted Conception,” Proc. of IEEE ISISE, 2012.

[27] Sánchez D, Batet M, Viejo A.” Detecting sensitive information from textual documents: an information-theoretic approach”. In: 9th International conference modeling decisions for artificial intelligence, MDAI 2012. Springer; 2012. p. 173–84

[28] J. Wang; F. Kang; X. Xu; J. Chen, "A Fast Single Pattern Matching Algorithm Based on the Bit-Parallel," Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on ,vol., no., pp.17-21, 18-22 Aug. 2010.

[29] Meystre SM, Friedlin FJ, South BR, Shen S, Samore MH. “Automatic deidentification of textual documents in the electronic health record:,” a review of recent research. BMC Med Res Methodol 2010;10.

[30] Pranay Yadav, Sweta Maurya, Shilpi Sharma “Internet of Things based Air Pollution Penetrating System using GSM and GPRS” 2018.

[31] Pranay Yadav, Saima Khan, Sandeep Kumar Shukla “Design and Analysis of Modified Truncated Flexible T Shape Patch Antenna with DGS for 5G and IoT Application” 09-11 May 2022.

[32] Pranay Yadav, Alok Upadhyay, V. B. Surya Prasath, Zakir Ali, and Bharat Bhooshan Khare “Evolution of Wireless Communications with 3G, 4G, 5G, and Next Generation Technologies in India” volume 709, 2021.

[33] Ritu Shrivastava; Abhigyan Tiwary; Pranay Yadav “Challenges Block Chain Technology Using IOT for Improving Personal and Physical Safety – Review” 08-09 January 2021.

[34] Pranay Yadav, Shachi Sharma, Prayag Tiwari, Nilanjan Dey Amira S. Ashour and Gia Nhu Nguyen “A Modified Hybrid Structure for Next Generation Super High Speed Communication Using TDLTE and Wi-Max” 2018

[35] Pranay Yadav, Nishant Chaurasia, Kamal Kumar Gola, Vijay Bhasker Semwan, Rakesh Gomasta & Shivendra Dubey “A Robust Secure Access Entrance Method Based on Multi Model Biometric Credentials Iris and Finger Print” pp 315–331, 01 January 2023.