International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# DigiSecure: Attribute-Based Document Transfer Solution

Trishna Panse[1]*, Prashant Panse[2], Reena Thakur[3], Priyanka Dudhe[4], Sudhir Shelke[5], Uma Patel[6]

**Submitted**: 28/05/2023 **Revised**: 06/07/2023 **Accepted**: 25/07/2023

**Abstract**: There are two examples of techniques for guaranteeing user credentials and facts secrecy are authentication and cryptosystems. Message Digest is used to check the uniqueness and accurateness of data traveling over an open channel due to its one-way nature. It recognizes unauthorized alterations and additions to broadcasts. When it comes to document uniqueness and creator oneness, digital signatures frequently use hashing. It is categorized as an attribute-based signature (ABS) and is updated by including new details about the attributes of the users. We looked at many historical approaches to the ABS phenomenon and identified some problems that needed to be handled. As a result, we came up with a solution that lowers the level of difficulty, usage, and operating expense while still enabling signature production and confirmation. We proposed an original DigiSecure: Attribute-Based Document Transfer Solution for Transporting Digital Document to highlight the approach of digital signatures using foundations and their initial reason. The system has policy-based access security limitations as well as adaptable primitives that offer signing authority total control over signature generation. It safeguards the secrecy of signatures and has a first order logic that is message-based. Various advantages were found after rationally studying the method, and these advantages will soon be proven by implementing the solution over the suggested outline under the given significant component.

***Keywords:*** *Data Security, MD, Digital_Signature, Rivest, Shamir, Adleman Algorithm, Signature Built on Features, X.509Certificate.*

## 1. Introduction

Cryptosystems are temporary systems for security of data and its protection that are set up to handle unauthorized solutions. All of the mathematically sophisticated representations are sufficiently strong to manage illegal access and changes. This is a mathematically challenging problem, and it is necessary to assume the complexity of the system, which is trackable and used as the primary building block for a security solution. Depending on the key used, cryptography systems are categorized as symmetric or asymmetric. Few instances of these cryptosystems include Data Encryption Standard and Advanced Encryption Standard, Rivest, Shamir, Adleman. Together, the cryptographic techniques triple DES, RSA, and MD5 are utilized to transmit data securely over Bluetooth. [16]. The mentioned cryptography systems' tools offer random visions for confirming the security of a goal. Subject to the restriction that the response is distinct for different inquiries, but it can be the same when the same notion is requested again, an arbitrary exposure replies to inquiries in an arbitrary manner. Two desirable characteristics of such an oracle are pre-image resistance and impact resistance [1-3]. To increase the practical approach to problem solving, one must adopt certain engaging instructional learning methodologies in order to comprehend the fundamentals of digital signature generation and verification. [17]. These cryptography systems' tools enable users to verify a goal's security in a variety of ways. Two desirable characteristics of such an oracle are pre-image resistance and collision resistance [1-3]. To understand the fundamentals of creating and verifying digital signatures and to enhance one's ability to solve problems practically, one must adopt certain engaging instructional learning techniques.

## 2. Materials and Methods

Due to their extensive client infrastructure, services, and hyper-visor virtualization technologies, internet applications are becoming denser. It offers consumers a service model that allows them to employ any computation paradigm based on a tenancy model to solve their problems The technique in mentioned paper [7] has been suggested since the problem is what such protection service area are supplied to end users in a desirable way. Evaluating security requirements is essential because Internet-based application service providers no longer guarantee the privacy of customer data. This is one of the additional elements of data security. Stages of security for each data object should be as follows:

Stage 1: Sending file over regular and encrypted set of rules.

Stage 2 involves access control for file, but without encrypting data inside.

Stage 3 involves access control techniques, such as encrypting the data inside data objects.

Stage 4: Access control techniques (including data and file encryption) and rights management tools (such as

*trishnapanse@gmail.com prashantpanse@gmail.com*
*rina151174@gmail.com priyankadudhe@gmail.com*
*sudhirshelke1976@gmail.com umapatel21@gmail.com*
*[1,2] Medi-Caps University, Indore, India, [3,4,6]Jhulelal Institute of Technology, [5]Guru Nanak Institute of Technology*

prohibitions on copying and publishing material without permission and date limits, etc.).

We have several security worries that many IT associations routinely ignore, which can greatly boost the risk of a protection breach spreading [4].

### Research gap in current system

### User Validation Not Enough

Predominantly with inventive common engineering methods that have been utilized just now, the standard username/password validation approaches are appallingly inadequate to prevent security breaches. Strong authentication is necessary and must be employed, and depending on a variety of background characteristics, different methods should be used. Physical tokens have been utilized regularly.

### Consistent User Access Authentication is insufficient

When a user changes roles or is promoted, for example, their access credentials are frequently no longer appropriate for the job at hand. Even while many organisations sometimes or sporadically verify a user's access permissions, this should be done formally, regularly, and through computerization so that it may be done quickly and unambiguously. Absence of a routine authorisation can make additional anomalies and violations of separation of functions more likely. [5].

### Absence of System Controls by Privileged Users

Confidential users frequently have more access than what is necessary for their tasks, which is a major cause of security breaches and issues. To carry out their duties, the aforementioned users need a wide range of access rights. [1].

### Control over the availability of information

Monitoring information access does not provide adequate protection or care. User also control how facts are used if one wants to stop it from being stolen or exposed. These weaknesses have contributed to the most obvious security mishaps in current memory.

### inadequate long-term user surveillance

Evidently, no one identify that some people was quickly downloading large amount of critical papers from military networks during the WikiLeaks attack. A thorough approach to observing user activity for ominous activity could help find many security vulnerabilities. As a result, one of the key causes of a high risk of security is the absence of efficient and constant user movement tracking. [13,14].

### Planned Work

An application that needs signatures of attribute and has particular requirements that no current cryptosystem can meet would be obvious to decipherers. With ABS, the user can create a stronger signature by supplying a subset of a list of properties. It makes use of the phenomena of anonymity to safeguard the privacy of each user's signature and uniqueness. This relates key overturning to attribute generation, which would improve ABS performance. This paper proposes a ground-breaking ABS architecture that solves all the problems and is also easy to use. It demonstrates an a better alternative to key turning employing a defined influence for handling user-selected attributes. In order to facilitate attribute negotiation, the considered order serves as a channel between the user and verifier. In order to create the signature, the handler asks the secret code sharing and a reverse check to ensure its originality and the necessary attributes. Here, key exchanges are carried out using the Rivest, Shamir, Adleman methods.

### Method

The process starts from development of a interested group of users in producing papers with digi signatures, as shown in Figure 1. The features and usage patterns of each user are related to a specific set of attributes. They were known as characteristics. The attribute collection contains these user attributes that have been extracted. The identification of Digidocs through signature was then confirmed using a data fragment from the user that contained all of the user's data through an attribute. This predicate logic is used by the hash algorithm to calculate the digest. MD is encrypted by sender private key and the RSA cryptosystem. The secure key will ensure the identity of user together with the user's qualities. Certificatex.509 is then added to save user’s validity data after encryption has been performed. The verification server verifies the data as part of an identity check. The system signs and stores all temporary data it creates in the repository. Which is used to recreate the signature. if the user produces a fresh document that calls for the identical signature. It also contains the predicate logic for signature generation. The signed message of the document is now sent across an unrestricted channel.

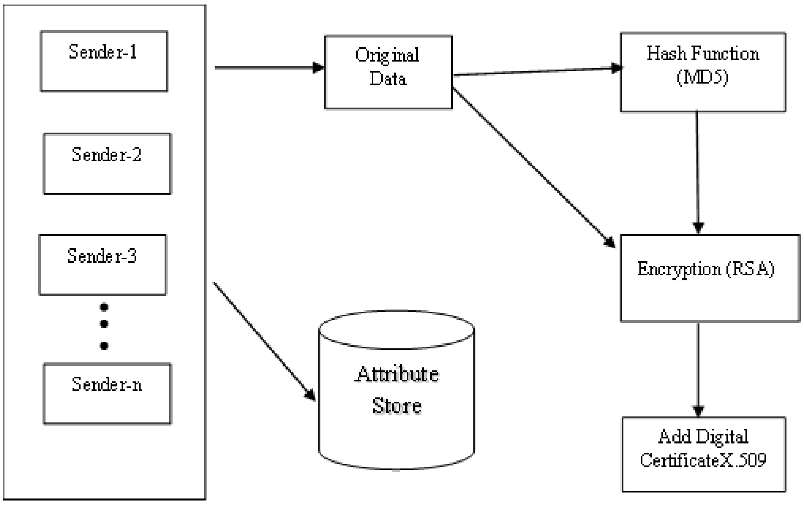


**Fig 1** Digital Signature Generation Process

The process of verification is the next stage of the suggested architecture, as depicted in Figure 2. The source of the hash linked to data portion is described at the beginning of this segment. PrivateKey of the generator, kept in public key repository, must be used to decode the digest before it can be extracted. Once the MD decrypted, the retrieved associated MD of data is used to recalculate message digest using the unique data. Along with the user's characteristics being authenticated, MD recalculation matched with already obtained. The authenticity of the sender's signature and the attribute of the user are established if they match. Finally, the message and a certificate with its confirmation are made available to the receiver.

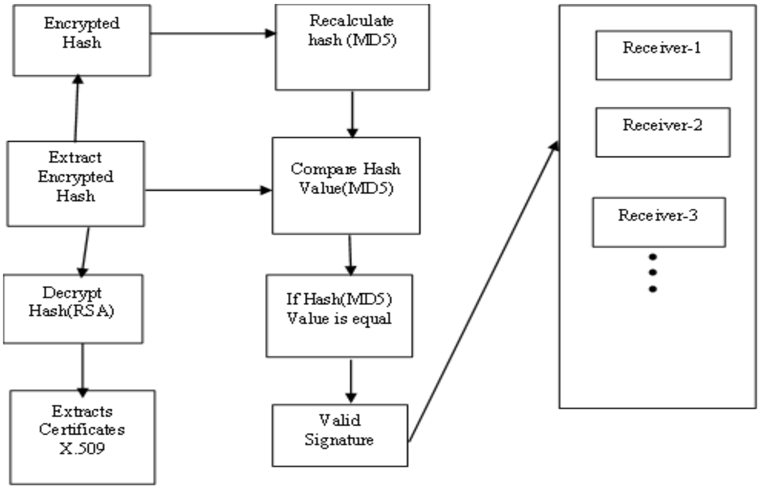
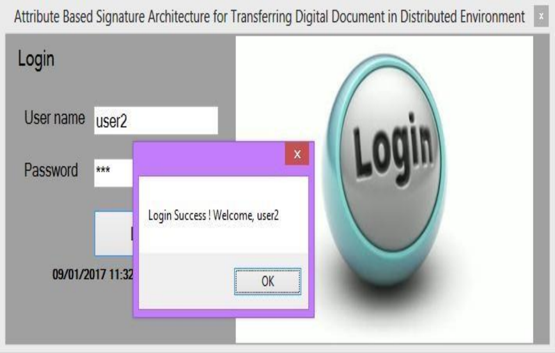


**Fig 2** Digital Signature Verification Process

## Execution

The first version of implementation needs validation as a fundamental measure security concern, seen in fig. 3. As a result, user must use the provided credentials to log into the system. Once the user's ID and password have been validated, a welcome message will appear.

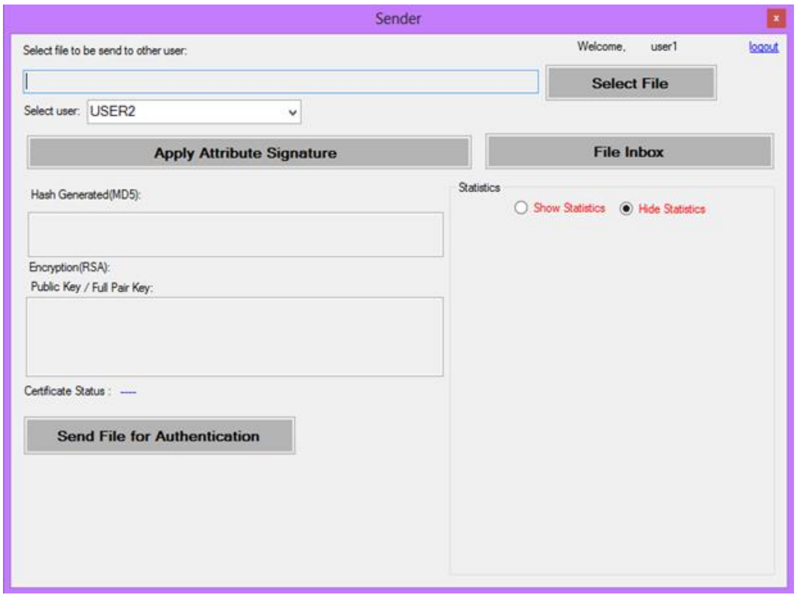

Attribute Based Signature Architecture for Transferring Digital Document in Distributed Environment
Login
User name
user2
Password
***
09/01/2017 11:32
x
OK
Login

Login Success ! Welcome, user2

**Fig 3** Login Screen

As seen in **Error! Reference source not found.** necessitates choosing files for secure sharing amongst the various system users. A set of user attributes will initially be generated by the ABS framework following the file selection in order to establish the user's identification based on their behavior. The MD5 hash algorithm receives these attributes in order to create the digest. The RSA encryption technique will additionally receive the user attributes when producing the key. The scheme create key pair, which is utilized as either a full key pair or a public key.

The X.509 certificate will be shown once the key has been produced. This certificate will include user, profile, file, and system-related information. A positive message is displayed for the file if the system and the properties it has chosen are accurate. The system is now prepared to securely exchange the file, as seen in Figure 5. Sending the file should proceed if the process and the resulting file are accurate.

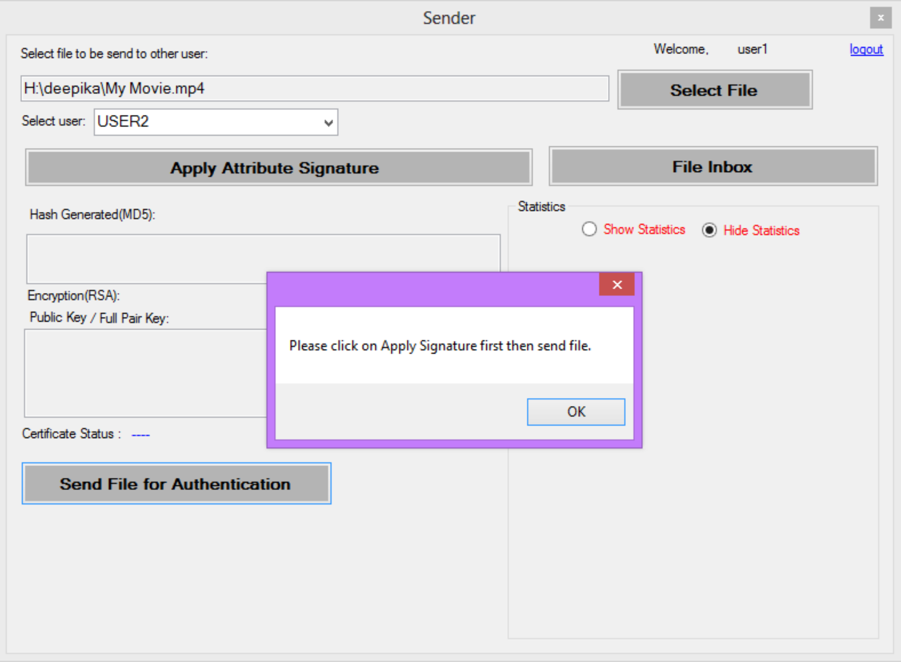

Sender
Select file to be send to other user:
Welcome, user1
logout
Select File
Apply Attribute Signature
File Inbox
Hash Generated(MD5):
Statistics
Encryption(RSA):
Public Key / Full Pair Key:
Certificate Status :
Send File for Authentication

Select user: USER2

○ Show Statistics ● Hide Statistics

Certificate Status : ----

**Fig 4** Core Panel of Attribute Signature


Sender
Select file to be send to other user:
Welcome, user1
logout
Select File
Apply Attribute Signature
File Inbox
Hash Generated(MD5):
Statistics
Encryption(RSA):
Public Key / Full Pair Key:
Send File for Authentication
OK

H:\deepika\My Movie.mp4

Select user: USER2

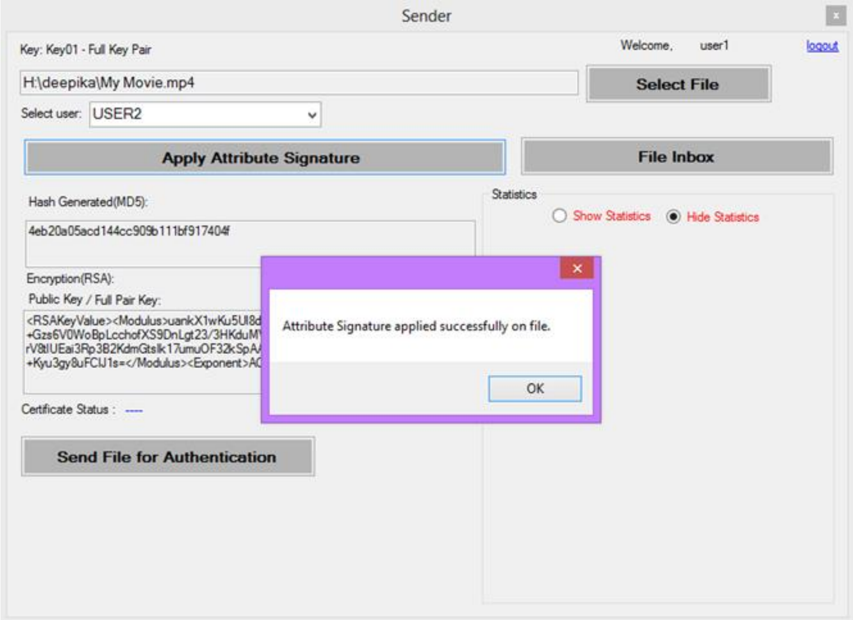
○ Show Statistics ● Hide Statistics

Certificate Status : ----

Please click on Apply Signature first then send file.

**Fig 4** Core Screen of Signature

The different sets of quantitative values, such as the times required to generate hashes, keys, and encryption keys, as well as the times required to deliver files and complete the entire process, are shown in Figure 6.



Key: Key01 - Full Key Pair

H:\deepika\My Movie.mp4

Select user: USER2

Hash Generated(MD5): 4eb20a05acd144cc909b111bf917404f

Encryption(RSA):

Public Key / Full Pair Key:

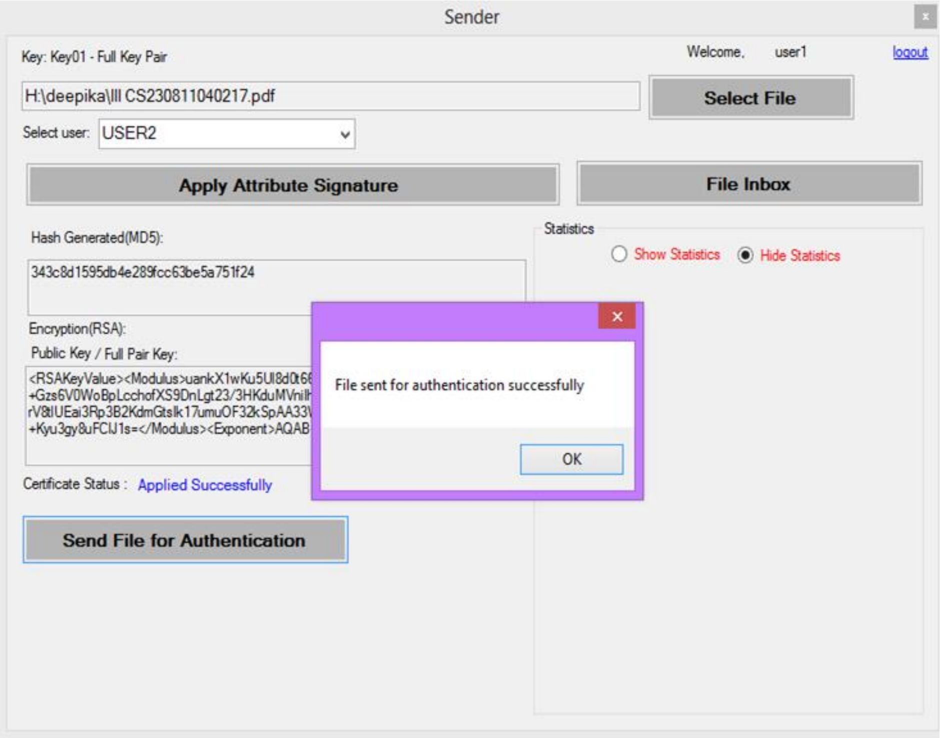
```
<RSAKeyValue><Modulus>uankX1wKu5UI8d
+Gzs6V0WoBpLcchofXS9DnLgt23/3HKduM
rV8tIUEai3Rp3B2KdmGtslk17umuOF32kSpA
+Kyu3gy8uFCIJ1s=</Modulus><Exponent>AC
```

Certificate Status : ----

Statistics: ○ Show Statistics ● Hide Statistics

Attribute Signature applied successfully on file.

**Fig 6** Successfully Signature Applied on File



Key: Key01 - Full Key Pair

H:\deepika\III CS230811040217.pdf

Select user: USER2

Hash Generated(MD5): 343c8d1595db4e289fcc63be5a751f24

Encryption(RSA):

Public Key / Full Pair Key:

```
<RSAKeyValue><Modulus>uankX1wKu5UI8d0t66
+Gzs6V0WoBpLcchofXS9DnLgt23/3HKduMVnilh
rV8tIUEai3Rp3B2KdmGtslk17umuOF32kSpAA33V
+Kyu3gy8uFCIJ1s=</Modulus><Exponent>AQAB
```

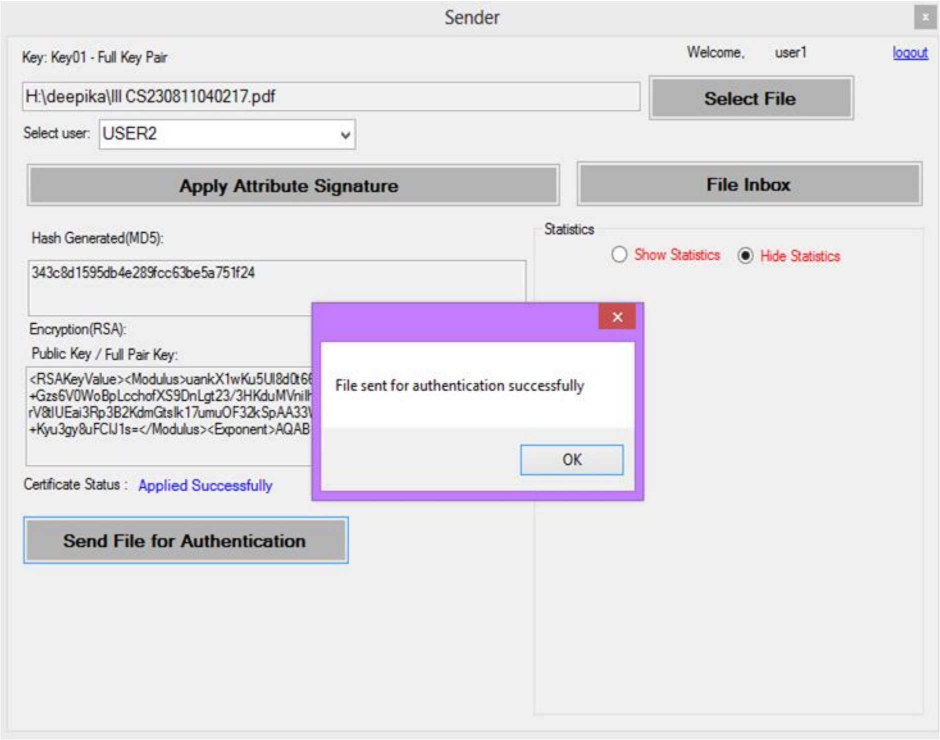
Certificate Status : Applied Successfully

Statistics: ○ Show Statistics ● Hide Statistics

File sent for authentication successfully

In

**Fig 5** clicked on Send button, data sent.



Key: Key01 - Full Key Pair

H:\deepika\III CS230811040217.pdf

Select user: USER2

Hash Generated(MD5):

343c8d1595db4e289fcc63be5a751f24

Encryption(RSA):

Public Key / Full Pair Key:

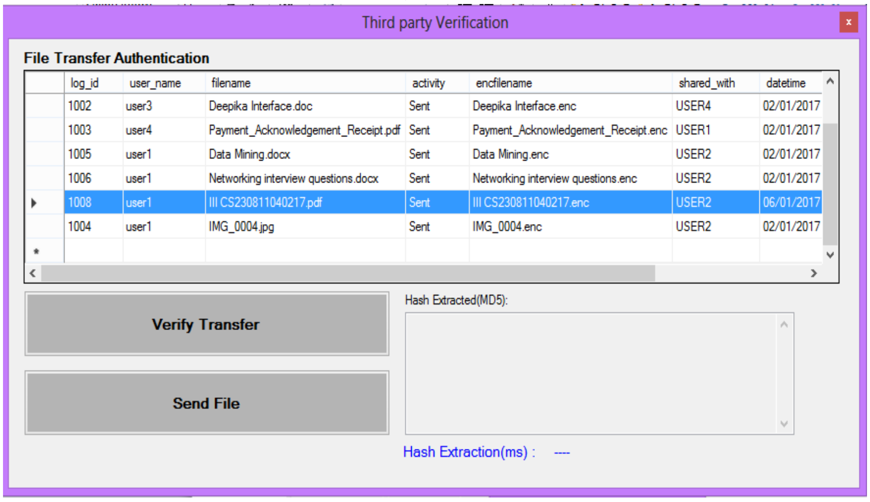
```
<RSAKeyValue><Modulus>uankX1wKu5UI8d0t66
+Gzs6V0WoBpLcchofXS9DnLgt23/3HKduMVnilH
rV8tIUEai3Rp3B2KdmGtsIk17umuOF32kSpAA33V
+Kyu3gy8uFCIJ1s=</Modulus><Exponent>AQAB
```

Certificate Status : Applied Successfully

File sent for authentication successfully

**Fig 5** Sent file Screen

Figure 8 depicts how files are received from various people. This will serve as a reverse step for the secure file transmission verification. This panel will display a list of the files that various people have sent. The verifier chooses any file from the list, applies the reverse procedure, and validates the sender. Integrity, authentication, and confidentiality were all guaranteed by this system



File Transfer Authentication

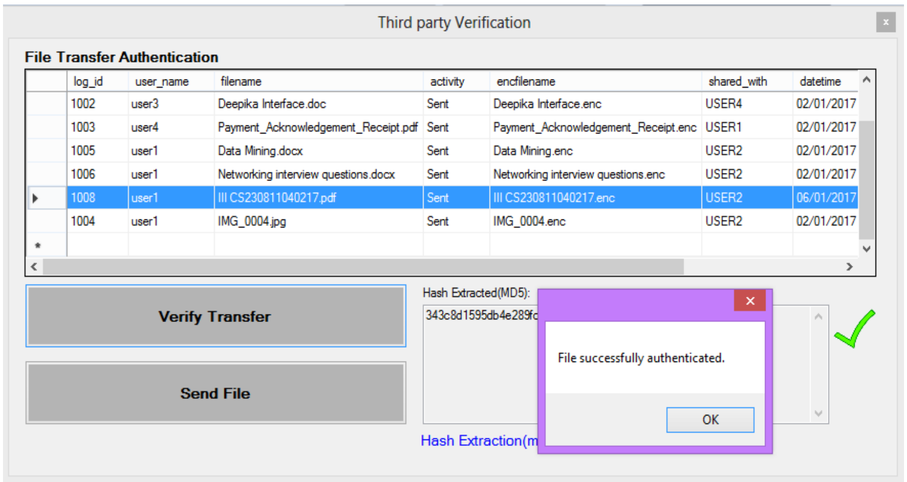
| | log_id | user_name | filename | activity | encfilename | shared_with | datetime |
|---|---|---|---|---|---|---|---|
| | 1002 | user3 | Deepika Interface.doc | Sent | Deepika Interface.enc | USER4 | 02/01/2017 |
| | 1003 | user4 | Payment_Acknowledgement_Receipt.pdf | Sent | Payment_Acknowledgement_Receipt.enc | USER1 | 02/01/2017 |
| | 1005 | user1 | Data Mining.docx | Sent | Data Mining.enc | USER2 | 02/01/2017 |
| | 1006 | user1 | Networking interview questions.docx | Sent | Networking interview questions.enc | USER2 | 02/01/2017 |
| ▶ | 1008 | user1 | III CS230811040217.pdf | Sent | III CS230811040217.enc | USER2 | 06/01/2017 |
| | 1004 | user1 | IMG_0004.jpg | Sent | IMG_0004.enc | USER2 | 02/01/2017 |
| * | | | | | | | |

Hash Extracted(MD5):

Hash Extraction(ms) : ---

**Fig 6** Third Party Verification Panel

Once the file has been confirmed, as illustrated in Figure 9, the verifier will send it to the selected receiver.


Third party Verification

File Transfer Authentication

| | log_id | user_name | filename | activity | encfilename | shared_with | datetime |
|---|---|---|---|---|---|---|---|
| | 1002 | user3 | Deepika Interface.doc | Sent | Deepika Interface.enc | USER4 | 02/01/2017 |
| | 1003 | user4 | Payment_Acknowledgement_Receipt.pdf | Sent | Payment_Acknowledgement_Receipt.enc | USER1 | 02/01/2017 |
| | 1005 | user1 | Data Mining.docx | Sent | Data Mining.enc | USER2 | 02/01/2017 |
| | 1006 | user1 | Networking interview questions.docx | Sent | Networking interview questions.enc | USER2 | 02/01/2017 |
| ▶ | 1008 | user1 | III CS230811040217.pdf | Sent | III CS230811040217.enc | USER2 | 06/01/2017 |
| | 1004 | user1 | IMG_0004.jpg | Sent | IMG_0004.enc | USER2 | 02/01/2017 |
| * | | | | | | | |

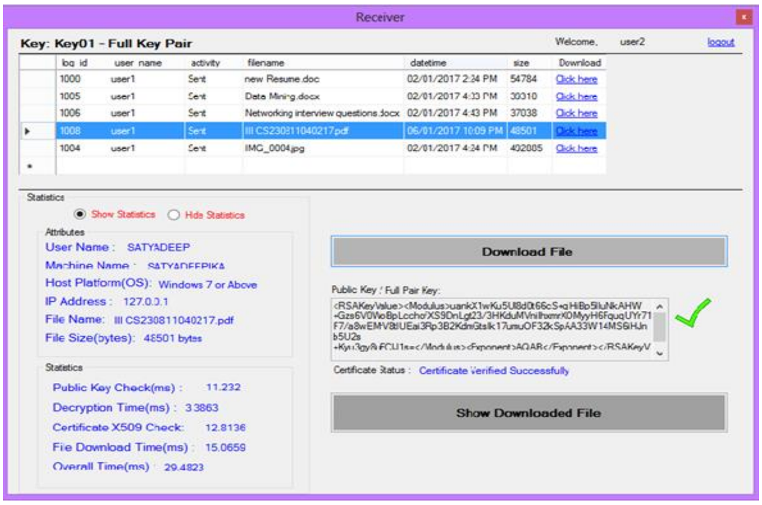
Hash Extracted(MD5):

343c8d1595db4e289fc

File successfully authenticated.

**Fig 9** Received Files of Third-Party Verifier

The file will be downloaded by the recipient, saved to local disc space, and allow to access. The procedure is depending on the administrators of his or her own efforts. As seen in Figures 10 and 11, this interface also presents the outcome attributes for collecting the quantitative values at various points in the data retrieval process. To obtain the correctness, efficiency, and reliability analysis, it primarily verifies the MD, characteristics, encrypt time, digest, certificate, and decrypt time employed using system.


Receiver

Key: Key01 - Full Key Pair

Welcome, user2

| | log id | user name | activity | filename | datetime | size | Download |
|---|---|---|---|---|---|---|---|
| | 1000 | user1 | Sent | new Resume.doc | 02/01/2017 2:24 PM | 54784 | Click here |
| | 1005 | user1 | Sent | Data Mining.docx | 02/01/2017 4:33 PM | 30310 | Click here |
| | 1006 | user1 | Sent | Networking interview questions.docx | 02/01/2017 4:43 PM | 37038 | Click here |
| ▶ | 1008 | user1 | Sent | III CS230811040217.pdf | 06/01/2017 10:09 PM | 48501 | Click here |
| | 1004 | user1 | Sent | IMG_0004.jpg | 02/01/2017 4:24 PM | 402005 | Click here |
| * | | | | | | | |

Statistics

● Show Statistics ○ Hide Statistics

Attributes

User Name : SATYADEEP

Machine Name : SATYADEEPIKA

Host Platform(OS): Windows 7 or Above

IP Address : 127.0.0.1

File Name: III CS230811040217.pdf

File Size(bytes): 48501 bytes

Statistics

Public Key Check(ms) : 11.232

Decryption Time(ms) : 3.3863

Certificate X509 Check: 12.8136

File Download Time(ms) : 15.0659

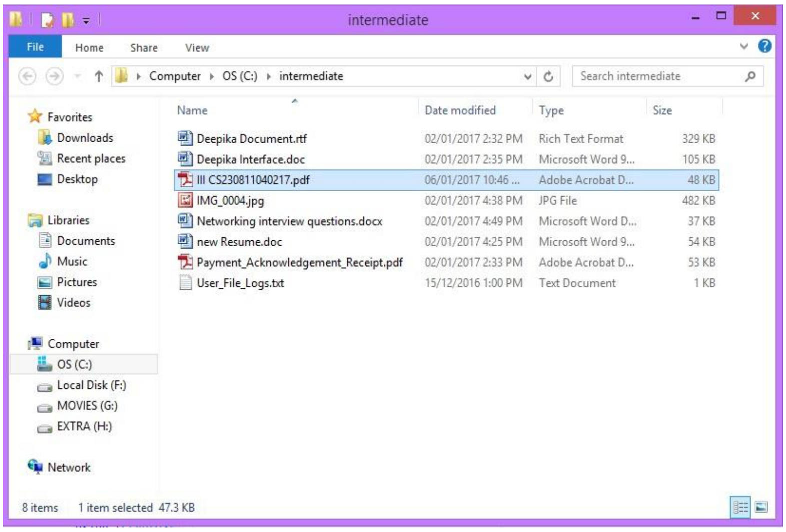
Overall Time(ms) : 29.4823

Public Key / Full Pair Key:

<RSAKeyValue><Modulus>uankX1wKu5U8d0t66cS+qHiBp5IluNkAHW
+Gzs6V0WoBpLccho/XS9DnLgt23/3HKduMVnlhxmrX0MyyH6FquqUYr71
F7/a8wEMV8tlUEai3Rp3B2KdnGtslk17umuOF32kSpAA33W14MS6HJn
b5U2s
+Kyu3gy8iFCU1s=</Modulus><Exponent>AQAB</Exponent></RSAKeyV

Certificate Status : Certificate Verified Successfully

**Fig10** Receiver Screen



| Name | Date modified | Type | Size |
|---|---|---|---|
| Deepika Document.rtf | 02/01/2017 2:32 PM | Rich Text Format | 329 KB |
| Deepika Interface.doc | 02/01/2017 2:35 PM | Microsoft Word 9... | 105 KB |
| III CS230811040217.pdf | 06/01/2017 10:46 ... | Adobe Acrobat D... | 48 KB |
| IMG_0004.jpg | 02/01/2017 4:38 PM | JPG File | 482 KB |
| Networking interview questions.docx | 02/01/2017 4:49 PM | Microsoft Word D... | 37 KB |
| new Resume.doc | 02/01/2017 4:25 PM | Microsoft Word 9... | 54 KB |
| Payment_Acknowledgement_Receipt.pdf | 02/01/2017 2:33 PM | Adobe Acrobat D... | 53 KB |
| User_File_Logs.txt | 15/12/2016 1:00 PM | Text Document | 1 KB |

**Fig7** File Received

## 3. Result

*We gathered data from the application of different types of files, user, size, OS. We could utilize a range of statistics to examine the advantages of the proposed strategy. as seen in the following table. These data will be used as records of user attributes.*

**Table *1***Many characteristics as display in table 1 that the algorithm uses to put the suggested solution into practice. According to their file type and size, each user in this table uses the application to create different file variations. Along with these vital details, we have also recorded the Internet Protocol address, platform, and system parameters. The attributes will be further handled in this

Table ***1***, which serves as the starting input, for the encryption, MD computation and DS.

**Table 1** User Attributes Records

| U _Name(Attribute Value 1) | Name of File (AttributeValue 2) | Size_AttributeValue 3 Bytes | System_Name (Attribute Value 4) | Platform (Attribute Value 5) | IP (Attribute Value 6) |
|---|---|---|---|---|---|
| User-1 | U_File_Log.txt | 296 | Medicaps | Windows10 | 127.0.0.1 |
| User-2 | Admi.docx | 14717 | Medicaps | Windows10 | 127.0.15.6 |
| User-3 | lic_4.jpg | 38001 | Medicaps | Windows10 | 127.62.24.52 |
| User-4 | Publication-1.doc | 124869 | Medicaps | Windows10 | 127.45.68.95 |
| User-5 | D_Mining.docx | 39315 | Medicaps | Windows10 | 127.86.32.47 |

In The stages listed in the suggested architecture of the approach make up the recommended algorithm, Attribute Based Signature Architecture, including message digest computation, key creation, RSA encryption, and finally uploading the processed document. The preceding table illustrates how the proposed Attribute Based Signature Architecture varies in how long it takes for various file types and sizes. Milliseconds (ms) are used to indicate the times that we measured for different heads.

**Table 2**, *We've compiled the statistics from the application's use of attribute-based signature in this table.*

*This table shows the total processing time (in milliseconds) as well as how long the suggested algorithm took to complete each phase. User characteristics listed in the*

**Table *1***table1 we implemented ABS.

The stages listed in the suggested architecture of the approach make up the recommended algorithm, Attribute Based Signature Architecture, including message digest computation, key creation, RSA encryption, and finally uploading the processed document. The preceding table illustrates how the proposed Attribute Based Signature Architecture varies in how long it takes for various file types and sizes. Milliseconds (ms) are used to indicate the times that we measured for different heads.

**Table 2** Communication Information

| NameofFile | SizeofFile | Fileid | Digest | publick | privatek | Digital Sign Gen | File Sent |
|---|---|---|---|---|---|---|---|
| D_Mining.docx | 39315 | 1052 | 34.452 | 2.089 | 1.062 | 2402.151 | 2297.020 |
| Third_sem_syllabus.pdf | 15985 | 1047 | 36.992 | 2.259 | 1.182 | 5259.562 | 2191.814 |
| R_Paper85695-700.pdf | 173619 | 1048 | 0.778 | 1.295 | 1.063 | 2254.593 | 2034.666 |
| Que_Networking.docx | 37040 | 1049 | 0.383 | 1.540 | 1.145 | 2034.082 | 1661.554 |
| R_Paper85695-700.pdf | 173618 | 1050 | 0.758 | 1.530 | 1.051 | 2396.673 | 1632.66 |

We try to discuss the time taken for extraction of an algo in **. We** have expected a data integrity and authenticity mechanism in this system using MD, Rivest, Shamir, Adleman algo and DS. To maintain data integrity, the technique states that we must generate MD and equivalence with previously produced. The authentication key for the file will then be determined as the next step. This table shows how long it will take to decrypt the file and recalculate the message digest. The file type and size that were shown in earlier tables are shown in this table.

**Table *3***. We have expected a data integrity and authenticity mechanism in this system using MD, Rivest, Shamir, Adleman algo and DS. To maintain data integrity, the technique states that we must generate MD and equivalence with previously produced. The authentication key for the file will then be determined as the next step. This table shows how long it will take to decrypt the file and recalculate the message digest. The file type and size that were shown in earlier tables are shown in this table.

**Table 3** Secure Extraction Statistics

| NameofFile | SizeofFile | Fileid | ExtractedDigest | publick Check | DigiSign Verify | receivedfile |
|---|---|---|---|---|---|---|
| D_Mining.docx | 39315 | 1052 | 34.452 | 9.384 | 2.283 | 9.514 |
| Third_sem_syllabus.pdf | 15985 | 1047 | 36.992 | 111.386 | 91.785 | 48.683 |
| R_Paper85695-700.pdf | 173619 | 1048 | 0.778 | 17.650 | 2.862 | 38.277 |
| Que_Networking.docx | 37040 | 1049 | 0.383 | 24.571 | 5.985 | 77.236 |
| R_Paper85695-700.pdf | 173618 | 1050 | 0.758 | 24.171 | 6.164 | 64.118 |

Along with the existing individual approaches, the **also provides** a qualitative analysis of the proposed Algorithm for the Attribute-Based Signature Architecture. The table shows how the system behaves when executing various file type, their size, and the amount of time needed for signature creation and verification. This table clearly shows how the suggested approach raises the block for subsequent security research. Combination approaches could be accurately analyzed with the addition of more examples and coequality testing, which is now not possible.

**Table *4*** also provides a qualitative analysis of the proposed Algorithm for the Attribute-Based Signature Architecture. The table shows how the system behaves when executing various file type, their size, and the amount of time needed for signature creation and verification. This table clearly shows how the suggested approach raises the block for subsequent security research. Combination approaches could be accurately analyzed with the addition of more examples and coequality testing, which is now not possible.

**Table 4** Comparing Qualitative Analysis to Current Practise

| **Method Name** | **Differences in Feature** | **Period** | **size** | **Involvedness** | **Competence** |
|---|---|---|---|---|---|
| Hash (Existing) | Single | High | Variable | High | High |
| RSA (Existing) | Single | Optimal | Variable | Low | High |
| Digital Signature (Existing) | Single | Low | Fixed | Low | Low |
| Certificate Generation (Existing) | Single | Optimal | Fixed | High | Low |
| **Proposed Architecture** | Multiple | Optimal | Variable | Low | High |

## 4. Conclusion

The method used to share information between parties affects how secure the data is. We must confirm the sender and the document after receiving documents that have been digitally verified in order to confirm their authenticity. It is related to the file. electronic signature. A new field uses the ABS approach to give the user more data security assurance and flexibility. In order to pinpoint certain unresolved problems, we examined how well several attribute-based signature techniques functioned. In general, these methods' resource requirements and computational complexity [5,11] are relatively high. To solve the issues, a creative approach is needed. We have put out a brand-new attribute-based signature architecture to overcome these problems.

## References

[1] Digital signing of original reports, By ALS Laboratories, Version 1 Published in 2010

[2] James H. Davenport and Dalia Khader, “Digital signatures: What you are versus \Who you are", in IACR Technical Review, 2010.

[3] S Sharmila Deva Selvi, Subhashini Venugopalan and C. Pandu Rangan, “A New Approach to Threshold Attribute Based Signatures”, in Theoretical Computer Science Laboratory Department of Computer Science and Engineering Indian Institute of Technology, Madras, 2010.

[4] Hemanta K. Maji, Manoj Prabhakaran and Mike Rosulek, Attribute-Based Signatures”, in Department of Computer Science, University of Illinois, Urbana-Champaign, 2010.

[5] Piyi Yang , Tanveer A. Zia , Zhenfu Cao and Xiaolei Dong , “Efficient and expressive fully secure attribute-based signature in the standard model”, Australian Information Security Management Conference, Edith Cowan University, Dec 2011.

[6] Javier Herranz, Fabien Laguillaumie, Benoit Libert and Carla Rafols, “Short Attribute- Based Signatures for Threshold Predicates”, in RSA Conference, San Francisco, United States, Springer, 2012.

[7] Fugeng ZENG, Chunxiang XU, Qinyi LI and Xiujie ZHANG, “Attribute-based Signature Scheme with Constant Size Signature”, in Journal of Computational Information Systems, ISSN: 2875–2882, Vol 8, Issue 7, 2012.

[8] Rupesh Vaishnav, “Attribute Based Signature Scheme For Attribute Based Encrypted Data In Cloud”, in International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181, Vol. 1 Issue 10, Dec 2012

[9] Feng Cai, Wangmei Guo and Ximeng Liu,“Threshold attribute based universal designated verifier signature scheme in the standard model”, in WSEAS Transaction on Communications, ISSN: 2224-2864, Vol. 13, 2012.

[10] Kefeng Wang, Yi Mu and Fuchun Guo, “Attribute-based signature with message recovery”, in Research Online Lecture Notes in Computer Science, University of Wollongong, 2014.

[11] Brinda Hampiholi, Gergely Alpaar, Fabian van den Broek, and Bart Jacobs, Towards Practical Attribute-Based Signatures””, in Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands, 2015

[12] Essam Ghadafi, ”Decentralised Traceable Attribute Based Encryption”, Presentation in University College London, April 2015

[13] Nigel Mc Kelvey , Kevin Curran and Nadarajah Subaginy , “The Internet of Things”, in IGI Global Journals, Category of Mobile and Wireless Computing, DOI: 10.4018/978-1- 4666-5888-2.ch570, 2005

[14] S. Sicari, A. Rizzardi, L.A. Grieco and A. Coen-Porisini, “Security, Privacy & Trust in Internet of Things: the road ahead”, in Preprint submitted to Elsevier, Feb 2015.

[15] Xiaofeng Chen, Jin Li, Xinyi Huang, Jingwei Li and Yang Xiang, Secure Outsourced Attribute-Based

Signatures"", in IEEE Transaction on Parallel and Distributed Systems, ISSN: 1045-9219, VOL. 25, NO. 12, Dec 2014.

[16] Vivek Kapoor et al." An Integrated Scheme based on Triple DES, RSA and MD5 to Enhance the Security in Bluetooth Communication" International Journal of Computer Applications 50(7):45-50, July 2012.

[17] Panse, P., Panse, T., Verma, R., Bhayal, D.K., Agrawal, A. (2019). An Edutainment Approach to Enhance Teaching–Learning Process. In: Kamal, R., Henshaw, M., Nair, P. (eds) International Conference on Advanced Computing Networking and Informatics. Advances in Intelligent Systems and Computing, vol 870. Springer, Singapore.

[18] Mr. Bhushan Bandre, Ms. Rashmi Khalatkar. (2015). Impact of Data Mining Technique in Education Institutions. International Journal of New Practices in Management and Engineering, 4(02), 01 - 07. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/35

[19] Leo, L. M. ., Simla, A. J. ., Kumaran, J. C. ., Julalha, A. N. ., & Bhavani, R. . (2023). Blockchain based Automated Construction Model Accuracy Prediction using DeepQ Decision Tree. International Journal on Recent and Innovation Trends in Computing and Communication, 11(1), 133–138. https://doi.org/10.17762/ijritcc.v11i1.6060

[20] Janani, S., Dilip, R., Talukdar, S. B., Talukdar, V. B., Mishra, K. N., & Dhabliya, D. (2023). IoT and machine learning in smart city healthcare systems. Handbook of research on data-driven mathematical modeling in smart cities (pp. 262-279) doi:10.4018/978-1-6684-6408-3.ch014 Retrieved from www.scopus.com