International Journal of Scientific Research in Engineering & Technology
Volume4, Issue2 (March-April 2024), PP: 67-76
https://www.doi.org/10.59256/ijsreat.20240402009
www.ijsreat.com
ISSN No: 2583-1240

Enhancing Electronic Services: Exploring the Optimal Security of Digital Signature Systems

V P Sushma[1], A Suresh Kumar[2]
[1]*M.E., Dept. of Biometrics and Cyber security, Rathinam Technical Campus, Coimbatore, TamilNadu, India.*
[2]*Assistant Professor, Department of Computer Science and Engineering, Rathinam Technical Campus, Coimbatore, Tamilnadu, India.*

To Cite this Article: *V P Sushma[1], A Suresh Kumar[2], "Enhancing Electronic Services: Exploring the Optimal Security of Digital Signature Systems", International Journal of Scientific Research in Engineering & Technology Volume 04, Issue 02, March-April 2024, PP: 67-77.*

Abstract*: E-government, e-learning, e-shopping, and e-voting are examples of electronic processes whose efficacy depends on the security, legitimacy, and integrity of the data that is sent back and forth between users. Sensitive material must be extensively vetted by its intended recipient and digitally signed by its original sender in order to meet these benchmarks. Digital signature systems, which are based on intricate cryptographic formulas, are necessary to guarantee the dependability of these electronic services. However, a number of variables, like key and block sizes, computational complexity, security settings, and modifications unique to a given application, affect how well these services function.*

The goal of the present research was to identify the ideal level of security for electronic mechanisms through a thorough investigation of industry-standard digital signature systems by the authors. They also looked into possible uses in many fields to improve comprehension and application in real-world situations.

Key Word: *EDMS, Digital Signature, HD5 algorithm, SHA algorithm.*

I.INTRODUCTION

With the rise of the Internet and continuous advancements in networking technology, an extensive array of personal, commercial, military, and governmental data is now readily accessible through global networking infrastructures. The increasing importance of network security arises from the ease with which intellectual property can be acquired and exploited via the internet.

The deployment of a network-based digital document security production system is one creative way to address these security issues. With the help of this technology, businesses can digitize paper documents and produce easily accessible electronic images for computer viewing. Due to the numerous advantages of switching from paper to digital formats, an increasing number of businesses are digitizing their files, manuals, catalogs, brochures, and other paper-based material.

Although handling paper records presents major obstacles, organizations have historically relied on paper filing systems for document storage and retrieval. Paper documents are difficult to handle effectively since they have to be kept and retrieved from a single area.

In addition to providing practical answers to the problems associated with conventional paper filing systems, electronic document management systems (EDMSs) significantly save operating costs for businesses. These platforms enable the archiving and retrieval of a wide range of digital documents, including word processing files, spreadsheets, databases, voicemails, emails, scanned photos, and HTML publications for the internet and intranet.

Systems for producing digital document security that are based on networks are designed to precisely record digital and analog data through the use of both conventional and unconventional electronic interfaces and protocols. After being recorded, this data can be examined, duplicated, and replayed as synchronized data streams, guaranteeing data security and integrity.

Authorization is the first step towards network security and usually involves usernames and passwords. It includes the rules and guidelines put in place by network administrators to protect against misuse, denial of service attacks, illegal access, and system alterations inside a computer network and its available resources. In essence, network security involves controlling who can access network data; network administrators are usually in charge of this task.

Network security, which determines which services are acceptable for network users, uses tools like firewalls to enforce access regulations, which are crucial for both individual computer users and enterprises. It's important to remember, though, that although firewalls are meant to stop illegal access, sometimes they can't identify potentially dangerous files like Trojan horses or computer worms that are sent across the network.

It's critical to understand that protecting the network as a whole is the most important consideration when talking about network security. Network security includes not only the protection of individual computers at each end of the communication chain but also the communication channels that are used to send data. Potential hackers could use any weakness in these channels

to their advantage in order to intercept data, decode it, and even implant fraudulent messages.

Therefore, protecting the network infrastructure is equally as crucial as protecting individual PCs and encrypting data. Network security measures must be implemented in order to stop and keep an eye on any unauthorized usage, modification, access, or denial of service within a computer network and its resources. Cryptography plays a key role in bolstering network security by encrypting and protecting critical data during transmission.

Threats to networks continue unabated even after many methods to strengthen security have been developed. In order to successfully address new threats and vulnerabilities, a great deal of research is still being done in the subject of network security.

Transforming signals to protect them from possible attackers is a science and an art form known as cryptography. It uses three different methods: symmetric key encoding, asymmetric key encryption, and hashing. Whereas symmetric-key encryption uses a single secret key for both encryption and decryption, asymmetric-key encryption uses two keys: a public key and a private key. Asymmetric encryption uses the recipient's public key to encrypt the communication, which the recipient decrypts with their private key. On the other hand, symmetric encryption uses a single key for both encryption and decryption.

Another crucial element of cryptography is hashing, which creates a fixed-length message digest from a variable-length message to guarantee data integrity. To ensure the integrity of the data, both this digest and the original message are sent.

Modern cryptography has advanced significantly since the 1970s, as seen by the creation of reliable encryption-based protocols and cutting-edge cryptographic applications. The National Bureau of Standards (NBS) released the Data Encryption Standard (DES) in January 1977, which was a significant milestone that elevated cryptography to the forefront of computing technology. The NBS's adoption of DES paved the way for in-depth study and advancement in the area.

Then, in December 1980, the American National Standards Institute (ANSI) adopted the DES algorithm, which became even more well-known and marked the entry of encryption into the business world. This action demonstrated the increasing significance of cryptographic methods for protecting sensitive data in a variety of industries.

Public Key Cryptography (PKC), a concept that is still undergoing extensive research and development, was proposed after another major turning point. PKC's debut broadened the applicability and power of cryptographic systems, creating new opportunities for safe data security and communication in the digital era.

It is true that cryptography, which is the study of guaranteeing the confidentiality, integrity, and legitimacy of communications, includes digital signatures. The practical application of methods to transform data or messages into a secure format that prevents unwanted access without the right key is known as cryptography.

Traditional paper-based workflows are quickly being replaced by electronic media in a variety of industries, including e-government and e-commerce, as technology continues to progress. To defend against hostile threats in modern digital settings, it is critical to preserve the security and sensitivity of digital objects. This emphasizes how crucial it is to put strong cryptographic safeguards in place, such as digital signatures, to guarantee the integrity and legitimacy of electronic communications and transactions.

An electronic version of a handwritten signature, known as a digital signature, is used to authenticate electronic documents. In actuality, compared to manual counterparts, digital signatures provide considerably more security. A public key encryption scheme is typically used by a digital signature to guarantee document integrity and confirm that it hasn't been altered.

The two main types of cryptosystems that fall under the umbrella of cryptography, a topic that bridges mathematics and computer science are symmetric and asymmetric. Data encryption and decryption in symmetric cryptosystems are accomplished with a single key, referred to as the secret key. Conversely, asymmetric cryptosystems, sometimes referred to as public key cryptosystems, encrypt data using a public key and decrypt it using a private key.

Symmetric cryptosystems provide a problem when it comes to safely distributing the secret key among users who want to protect their communications or data. In order to overcome this difficulty, public key cryptosystems produce both the public and secret keys using cryptographic algorithms. DES and the reliable RSA algorithm are two notable algorithms.

The RSA algorithm, created in 1977 at the Massachusetts Institute of Technology by Ron Rivest, Adi Shamir, and Leonard Adleman, is one of the most used public key cryptosystems. It entails choosing another huge integer, known as the encryption key, and multiplying two large, randomly selected prime numbers to create a public key. The encryption key and the result of multiplying the two prime numbers make up the public key.

Using this public key, Ron Rivest came up with a technique to jumble communications, turning plaintext into cipher text. A decryption key, which is necessary for decryption, can only be calculated with the use of the original prime numbers. By using this decryption key, the cipher text can be broken down and returned to plaintext. The RSA algorithm's strength is its mathematical complexity, which makes it very challenging to figure out the original prime numbers and encryption key.

Phil Zimmermann created Pretty Good Privacy (PGP), a well-known public key cryptosystem, in the early 1990s. The length of the keys that are used to encrypt and decrypt data or communications directly affects their security. Longer keys are generally more powerful. For example, a 128-bit key is more secure than a 256-bit or 1024-bit key, and a 56-bit key is not as strong as a 128-bit key.

Public Key Encryption (PKE) uses two keys: a private key that is used only by the user and is secured by a password that they have carefully selected, and a public key that is used by other users. Public key servers are frequently used to store public keys. One of these keys can only be used to encrypt a document; the other key in the pair is required to decrypt it.

Similar to handwritten signatures, digital signatures are used as an authentication mechanism anywhere data authentication is needed. The idea of digital signatures was first introduced with the development of public-key cryptosystems. In essence, a signer creates a signature by digitally signing a document using their private key. A verifier receives this signature, the document, and the signer's public key after that. With the matching public key, the verifier can determine whether the signature is

legitimate. Every person involved must register their public key with a central authority, called the Certificate Authority, in order to guarantee trust in the public keys.

Digital signatures function similarly to handwritten signatures as an authentication tool anywhere data authentication is needed. Digital signatures were first established with the introduction of public-key cryptosystems. A signer essentially uses their private key to digitally sign a document, creating a signature. After that, a verifier receives this signature, the document, and the signer's public key. The associated public key can be used by the verifier to determine whether the signature is legitimate. Each participant in the process needs to register their public key with the Certificate Authority, a central authority, in order to guarantee public key trust.

Hash functions are essential for guaranteeing the security of data on the internet. In particular, a variety of security-related applications use cryptographic hash functions. These functions produce a message digest, which is a fixed-size output, from arbitrary-length data inputs. They are made to ensure message integrity, which allows the recipient to identify any changes made to the message after it has been sent and before it has been received by the intended recipient. As such, any message that has been altered can be ignored.

Applications for this hash function integrity property can be found in a number of domains, such as the production of random numbers and digital signatures. It's important to remember that a lot of hash functions, including SHA-1, SHA-2, SHA-3, and MD-5, depend on the Merkle-Damgård architecture and could not be totally safe from assaults. Several possible attacks on this structure are discussed in the study, which also puts these hash functions at danger.

Digital signatures also use cryptographic hash algorithms. The hash code is compared by the sender and the recipient during the authentication process to confirm its legitimacy. If the message that the recipient retrieves matches the one that the sender originally signed, it is considered legitimate. Any changes made to the data will inevitably affect the hash code that is sent with the data, warning the recipient of possible manipulation.

II.LITERATURE SURVEY

A. The Network Security and Intrusion Detection System

R. Dharmarajan and V. Thiagarasu created a network security framework in 2019 that starts with authorization and usually requires a username and password. Their work was published in [1]. In order to prevent and manage unauthorized access, system alterations, misuse, and denial of service attacks against a computer network and its resources, network administrators set in place a variety of rules and regulations that collectively constitute network security. At its core, network security is about controlling who can access data on a network; this is the network administrator's job. This is a feature that is becoming more and more important for both individuals and companies.

A firewall reduces the possibility of unwanted system entry by enforcing access restrictions that specify which services are acceptable for network users to access after they have been granted authorization. Firewalls, however, occasionally might not be able to identify potentially dangerous material, such Trojan horses or computer worms, that is sent across the network. Intrusion detection systems (IDS) and anti-virus software work together to detect and neutralize malware threats in order to address this.

In addition, modern network security techniques include anomaly monitoring, which entails examining network traffic with programs such as Wire shark and keeping logs for further high-level analysis and auditing. Furthermore, encryption is frequently used to protect privacy policies when two hosts are communicating across a network.

B. Network Security and Cryptography

A network security framework was proposed in 2014 by Dr. H S Guruprasad et al. [2]. It consists of rules and guidelines that network managers have created to stop and keep track of any unauthorized access, misuse, modification, or denial of a computer network or its resources. A key component of network security is cryptography, which is a basic method of data protection.

The science and art of converting messages to make them safe from attackers is known as cryptography. It includes hashing, symmetric-key encoding, and asymmetric-key encoding as its three main techniques. Asymmetric-Key Encryption uses two keys: a public key and a private key, whereas Symmetric-Key Encryption uses a single secret key for both encryption and decryption. Using the recipient's public key, the sender encrypts the data, and the recipient uses their private key to decrypt the message.

Another crucial cryptographic method is hashing, which is the process of creating a fixed-length message digest from a variable-length message. Data integrity is ensured by transmitting both the message and the digest, which confirms that the received message has not altered.

These cryptographic techniques work together to provide strong protection against unwanted access and guarantee the confidentiality, integrity, and validity of data that is transferred. Together, they constitute the cornerstone of network security.

C. Online Electronic Documents based on Novel Techniques

In 2024, Pritesh Shah and colleagues [3] presented the concept of encryption technology, realizing its growing importance in protecting digital information that are accessible online. The increasing difficulties and complexity of document verification—which frequently proves to be laborious and time-consuming when utilizing current techniques—was the driving force for the study.

Conventional encryption systems, such Rivest Shamir, Adleman (RSA), Data Encryption Standard (DES), and AES, may have drawbacks when used separately to meet specific client needs. As a result, the study suggests hybrid cryptography,

which incorporates two novel algorithms into the encryption protocols already in place.

A digital signature is created for user data upon upload. After that, the data are encrypted in parallel using the suggested Secured Hash Function-265 (SHA-256) technique in conjunction with RSA and enhanced DES (SHA-256 + Enhanced DES + RSA). Using a hybrid approach, possible weaknesses related to specific encryption methods are mitigated and document encryption security and efficiency are improved.

D. **Secure Hash Algorithm with its variants**

A 2017 study work by Dr. S. M. Ghosh et al. [5] focused on comparing different secure hashing algorithms and their corresponding variants. The time needed to calculate the hash value is used to evaluate each algorithm. Finding the algorithm that requires the least amount of time to compute hashes is the aim.

The authors suggest that double hashing be used as a future project. This is the process of augmenting the security of data transferred through cloud services by fusing the most effective secure hashing algorithm with another. These algorithms produce fixed-size output strings from arbitrary data blocks that are fed into them. Whether the modifications are deliberate or unintentional, even little adjustments to the input data result in drastically different cryptographic hash results. The hash value is known as the message digest, while the input data is commonly referred to as the message.

One prominent example is the Secure Hash Algorithm (SHA), which is utilized for message authentication, data integrity verification, and digital certificates. The U.S. Federal Information Processing Standard (FIPS) for digital signature applications, SHA was created by NIST (National Institute of Standards and Technology) and acts as a fingerprint that is unique to the data.

E. **Secure Digital Signature Schemes based on Hash Functions**

In 2014, notable progress was made in the fields of communication and information technologies by Patel Prachi Pravinumar et al. [6]. Electronic media quickly supplanted paper-based workflows during this time, especially in systems like e-government and e-commerce where all forms and data are handled digitally. But in these systems, it became crucial to protect digital objects' security and sensitivity from malevolent actors.

The significance of hashed messages in mitigating man-in-the-middle attacks, a common danger to digital signatures, was emphasized by the researchers. Digital signatures, in contrast to handwritten ones, are unchangeable once signed because their integrity is based on the signed document itself. Unlike other algorithms that require more complex operations, the suggested technique for digital signatures is renowned for its efficiency, requiring simply logical operations like OR and XOR. Additionally, there are fewer hardware complexity constraints for components like as Application-Specific Integrated Circuits, Logic Devices, and Programmable Gate Arrays.

The goal of digital signatures is to imitate the authenticity and verifiability of handwritten signatures. In this case, a subliminal channel's bandwidth—a measurement of its ability to transmit hidden information—is extremely important. Testing the new algorithms produced encouraging results: for messages under 1600 bytes, the hashed file size was 4% smaller than the original file. These results show how effective and efficient the suggested method is at improving the security and integrity of digital signatures.

F. Cryptography and Network Security

In [7], Daniel Lloyd Calloway et al. carried out an extensive analysis of studies that were released in 2008 concerning cryptography in relation to network data and international communications security. The study clarifies the place of cryptography in the present and future security environments by contrasting and comparing previous studies to pinpoint broad trends in this area.

The paper explores the role that cryptography plays in protecting people, businesses, and other organizations in the current era of networking, computing technologies, and web-based e-commerce. The goal is to support further cryptography research and development by looking at both scholarly and non scholarly publications. It claims that these initiatives are essential to maintaining the security and privacy of electronic data and to enabling the global expansion of e-commerce companies through safe online transactions.

I. Digital document security and authenticity

As part of the Digital India Programme, Gajanan Badhe created a Digital Locker in [16] with the goal of reducing dependency on physical papers and facilitating the interchange of electronic data among agencies. E-documents can be shared via registered repositories through this portal, guaranteeing their legitimacy on the internet. Additionally, residents can securely share their electronic documents with government agencies and other groups by uploading them and digitally signing them with the e-sign feature.

The Digital Locker initiative by the Government of India, launched by the Department of Electronics and Information Technology (DeitY), offers several key features:

- Digital empowerment of residents with cloud-based Digital Locker.
- Enablement of e-Signing of documents for electronic availability and online sharing.
- Reduction in the usage of physical documents.
- Assurance of e-document authenticity, thereby eliminating the use of fake documents.

- Secure access to government-issued documents through a web portal and mobile application.
- Reduction in administrative overhead for government departments, simplifying service delivery.
- Anytime, anywhere access to documents for residents.
- Adoption of open and interoperable standards for easy document sharing across departments and agencies.
- Ensuring privacy and authorized access to residents' information.

To further meet the demands of its clients for the safe and convenient storage of critical documents, ICICI Bank also provides the e-Locker document storage option. Documents are kept safe and only accessible with a secure login through an ICICI Direct account or ICICI Bank Internet Banking, thanks to the e-Locker. This feature ensures security and convenience of retrieval by giving users access to their papers at any time and from any location.

Additionally, Kleeto offers a document storage system that offers options for both digital and analog data storage. It provides a safe digital repository for papers, enabling immediate access to crucial files upon logging in. Intelligent indexing and customizable restricted access to certain users are two elements of Kleeto's digital locker that improve security and usability.

J. Electronic Document Protection System with Illegal diffusion

In [17], Quan-xing presented a unique solution that combines Digital Rights Management (DRM) and digital fingerprint technology to improve document security while taking into account the requirements of authorized users. The system presents a methodology for electronic document protection that is intended to pinpoint user accountability in the case of unauthorized document disclosures.

The architecture of the system, which consists of the Document Distributing End, Distribution Server, Digital Fingerprint Server, DRM Server, and Document Using End, is designed to provide thorough document management and protection.

1. Document Distribution End: Produces a document license that describes guidelines for document security and administration. The license is sent to the DRM Server following identity confirmation.

2. Fingerprint Encoding System, Fingerprint Tracking System, and Third Party comprise the Digital Fingerprint Server. By encoding user identity data that was sent by the Document Distribution End, this server inserts the encoding sequence—which functions as the user's signature—into the original document.

3. Distribution Server: Centralized platform to distribute DRM materials, guaranteeing users receive them only via approved routes and guarding against illegal access.

The following workflow is used by the system to function:

- A document license is created by the Document Distributing End and sent to the DRM Server.
- The Digital Fingerprint Server encodes user identifying data and embeds it into the original document.
- A copy of the document is transformed and encrypted by the Document Distributing End, turning it into a DRM document that is then sent to the Distribution Server.
- The Document Using End guarantees adherence to identity verification protocols by authenticating the user and granting access to the necessary DRM document.

While Quan-xing's system integrates digital fingerprinting in a unique way to improve security and accountability in document distribution and usage, it is similar to traditional DRM-based electronic document protection systems in other aspects as well, such as license generation, document conversion, encryption, and authentication.

III.METHODOLOGY

A. Existing System

The main limitation of this approach lies in the lack of quick and convenient access to files when needed. The expenses linked with storage fees, coupled with the inconvenience of off-site storage, could surpass the initial budget estimates of your organization. Furthermore, despite being stored electronically, these files are still susceptible to the same risks as physical documents.

B. Drawbacks of the Existing System

Vulnerable to small-scale image manipulation: There's a chance of losing data stored in the Least Significant Bits (LSBs) when converting an image from a format like GIF/BMP, which maintains the original image exactly (lossless compression), to a JPEG format, which doesn't (lossy compression), and then back again.

Sequential LSB modification is easily identifiable since it produces a statistical pattern that differs from the image's unaffected areas.

IV. PROPOSED SYSTEM

This method's unobtrusive buried text prevents attention-grabbing, which is advantageous. It remains undetectable as it blends in perfectly with harmless information, such as a video. Subtle colour value changes make it possible to send tiny pieces of information that are almost impossible to intercept.

Advantages of Proposed System

Proposed Scheme tries to improve the security of the data.

- Robustness.
- Increased manifold.

- The method hides one image in another image and works with 24bit bitmapcolor image.
- Security of the hidden communication.

V.SYSTEM ARCHITECTURE

Admin

In this module the admin login details are maintained. Admin is used unique user name and password. They are only access in this module.

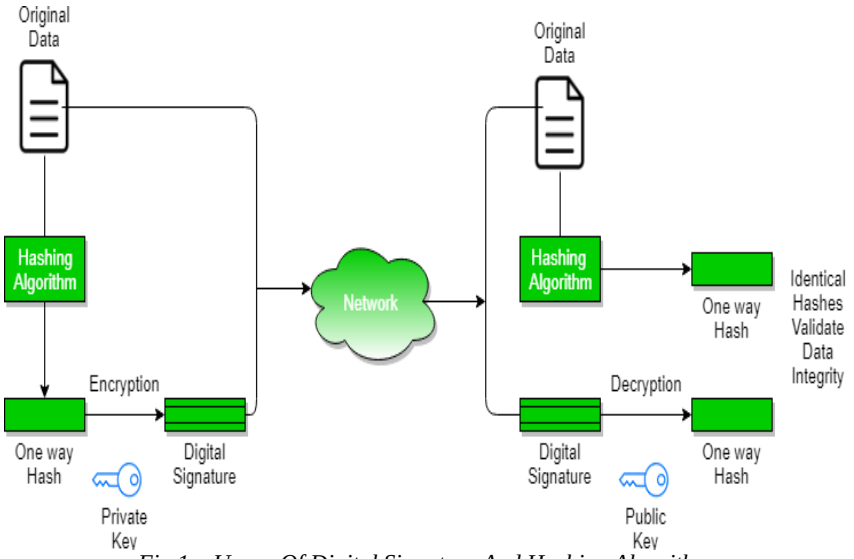

Fig 1 – Usage Of Digital Signature And Hashing Algorithm
Hashing Algorithm

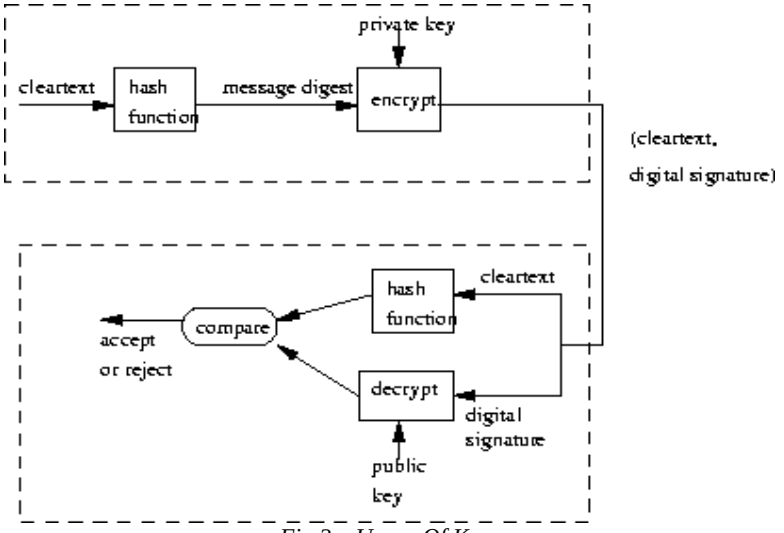

Fig 2 – Usage Of Keys

VI.MODULE DESCRIPTION

File Sending and Receiving

Socket-based file transmission and receiving is a crucial capability for data transfer between systems. This tool makes it easier for computers linked to a network to share a variety of file kinds with one another. It functions by creating a connection over a TCP port between two computers, one of which is in the Passive mode and waiting for connections, and the other of which is in the Active mode and starts the connection by providing the Passive computer's IP address.

Convert to Digital Format

Digital documentation refers to the process of transforming traditional text documents into digital formats accessible via electronic devices such as computers. This conversion entails creating electronic versions of the original text documents, allowing them to be viewed and accessed digitally. The transition to digital documentation offers numerous advantages, prompting a growing number of companies to convert their textual data, including files, manuals, catalogues, brochures, and other textual

content, into digital formats.

Convert to Analog Format (Original Document)

This module gives you the ability to designate a file name for digital data storage and the extraction of the analog file (original document) that corresponds to it. The data in this file are compiled with their corresponding characteristics to produce a logical unit that the user has selected for reference. This idea comes up a lot when people are talking about information management.

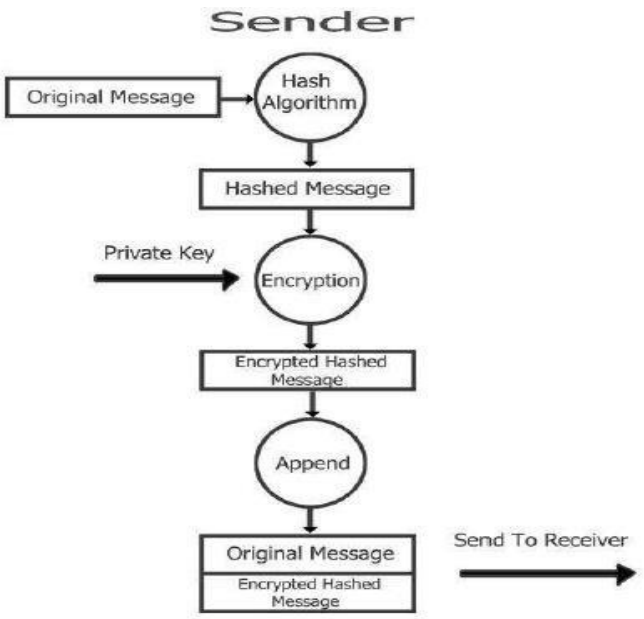

Fig 3-Operation of Sender

VII.IMPLEMENTATION

The crucial stage of a project where the conceptual design is turned into a working system is called implementation. The main goal is to successfully implement the new system and give consumers confidence in its efficacy and efficiency. This phase includes a number of crucial elements, such as:

- Testing a developed program with sample data
- Detection and correction of error.
- Making necessary changes as desired by users.
- Training user personal.

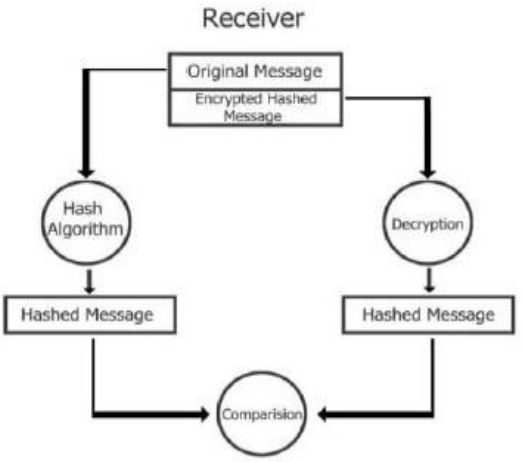

Fig 4 – Operation of Receiver

Comparision of Hash Algorithm in Digital Signature

Digital signature creation heavily relies on cryptographic hash functions. Both the sender and the recipient compare the hash codes during the authentication procedure to guarantee the accuracy of the data. The message is deemed legitimate if the hash codes match. The hash code is delivered with the data and is updated in response to any changes made to the data.

MD5 Algorithm

Digital signature creation heavily relies on cryptographic hash functions. Both the sender and the recipient compare the hash codes during the authentication procedure to guarantee the accuracy of the data. The message is deemed legitimate if the hash codes match. The hash code is delivered with the data and is updated in response to any changes made to the data.

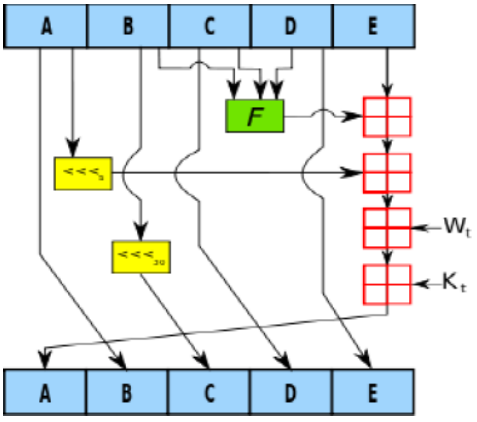

Fig 5 – One Operation of Md5 Algorithm

SHA-0

SHA-0 is a 160-bit hash algorithm that was first released as "SHA" in 1993. However, a "significant flaw" that remained revealed led to its rapid withdrawal from use shortly after it was published. As a result, the somewhat altered version known as SHA-1 took its place.

SHA-1

Similar to MD4 and MD5, SHA-1 uses similar techniques to construct a message digest. One bitwise rotation in the message scheduling of its compression function is the main distinction between SHA-1 and SHA-0. A message digest, or 160-bit hash value, is the result of SHA-1. There are 40 digits in the hexadecimal representation of this hash value.

Step1:- Bits padding:-Add Padding to the end of the genuine message length is 64 bits and multiple of 512.

Step2:- Appending length: - In this step the excluding length is calculated.

Step3:- Divide the Input Text into 512-bit blocks :- We divide the input in the 512 bit blocks

Step4:-Initialize chaining variables. In this step we initializing chaining variables here we initialize 5 chaining variables of 32 bit each=160 bit of total.

Step5:-Process Blocks

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

$\oplus, \wedge, \vee, \neg$ denote the XOR,AND,OR and NOT operations respectively.

Fig 6 – One Operation of SHA 1 Algorithm

1. Copy the chaining variables
2. Divide the 512 into 16 sub blocks
3. Process 4 rounds of 20 steps each SHA-1: The Function H Compression function operates as follows:

Each round has 20 steps which replaces the 5 buffer words (A,B,C,D,E) with:(E + f(t,B,C,D) + (A << 5) +Wt +Kt),A,(B <<30),C,D)

- t is the step number
- f(t,B,C,D) is nonlinear function for round
- Wt is derived from the message block
- Kt is a constant value derived from sin

SHA-1 forms part of several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME, and IPsec. SHA-1 hashing is also used in distributed revisioncontrol systems.

SHA-2 Algorithm (Secure Hash Standard)

A secure hash algorithm is known as SHA. With several enhancements over SHA-1, SHA-2 is a major advancement. It consists of a family of hash functions for cryptography, such as SHA-224, SHA-256, SHA-384, and SHA-512, that were created by the National Security Agency (NSA) and included in the U.S. Federal Information Processing Standard in 2001 by the National Institute of Standards and Technology (NIST). SHA-2 and SHA-1 are comparable, however SHA-2 has not been

vulnerable to the same attacks that SHA-1 was. The new hash function known as SHA-3 was chosen as the winner of the 2012 NIST hash function competition.

Significant improvements over SHA-1 are brought about by SHA-2. The hash functions SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256 are all part of the SHA-2 family. Novel hash algorithms called SHA-256 and SHA-512 are calculated using 32-bit and 64-bit words, respectively. Their structures change only in the number of rounds, otherwise they are essentially similar, despite using different shift amounts and additive constants. Shorter versions of SHA-256 and SHA-512, respectively, are SHA-224 and SHA-384, which are calculated with different starting values. In a similar vein, SHA-512 is truncated in SHA-512/224 and SHA-512/256.

Both the DKIM message signing standard and the authentication procedure for Debian software packages use SHA-256. SHA-512, on the other hand, is used in a system intended to verify historical video footage from the International Criminal Tribunal for the genocide in Rwanda. It is advised to utilize both SHA-256 and SHA-512 with DNSSEC. Furthermore, 256-bit and 512-bit SHA-2 is being used by Unix and Linux providers for safe password hashing.

$$Ch[E,F,G] = [E \wedge F] \oplus [\neg E \wedge G]$$
$$Ma[A,B,C] = [A \wedge B] \oplus [A \wedge C] \oplus [B \wedge C]$$
$$\sum_0 (A) = [A \ggg 2] \oplus [A \ggg 13] \oplus [A \ggg 22]$$
$$\sum_1 (E) = [E \ggg 6] \oplus [E \ggg 11] \oplus [A \ggg 25]$$

Fig 7 – Iteration in the Sha 2 Algorithm

For SHA-512, the bitwise rotation uses different constants, while the given values are for SHA-256. The green sign in Figure 5 denotes an addition modulo 2^32. Secure hash algorithms SHA-1 and SHA-2 are legally required for use in a number of U.S. Government applications. These applications include the protection of sensitive unclassified data through the use of these algorithms in different cryptographic protocols and methods. The adoption and use of SHA-1 by private and commercial enterprises was promoted by FIPS PUB 180-1. SHA-1 isn't often used in most government applications, though.

Comparison of Hashed Algorithms (MD5 and SHA2)

While SHA-2 generates outputs of different lengths, such as 32 bytes (256 bits) for SHA-256 and 64 bytes (512 bits) for SHA-512, the MD5 algorithm yields an output size of 16 bytes(128bits).

Padding is used in the first processing step to make sure the message length is more than 512 bits. This is appending one '1' bit, then a sequence of '0' bits, with the length of these extra bits changed to satisfy the 512-bit demand. In order to guarantee that the message length affects the hash calculation, the actual message length is also encoded in a 64-bit format and appended to the end of the message.

These methods have an O(n) time complexity, where 'n' is the length of the input message, because of their fixed output sizes.

TABLE I
COMPARISON OF HASH ALGORITHM

Algorithm	Methodology	Output	Time Complex	Performance
MD5	Divide to 512b, 64 times loop	32B	O(n)	Collision After 2006
SHA2	Divide to 512b, 64 times loop	64B	O(n)	Without collision

TABLE II
COMPARISON OF LOGICAL OPERATIONS, CURRENT STATUS AND HARDWARE COMPLEXITY

Algorithm	Logical operations	Current status	Hardware complexity
MD5	AND,OR,NOT,Rotating shifts	Collision	Medium
SHA2	AND,OR,NOT,Rotatingshifts,XOR	Running	Large

Preventing man-in-the-middle attacks is essential for preserving the integrity of digital signatures in the context of hashed messages. One important feature of digital signatures is that, once they are signed, they cannot be altered. This sets them apart from handwritten signatures, whose legitimacy depends on the integrity of the signed document. We examine hashed algorithms by contrasting their logical operators with the hardware complexity, as shown in Table II.

Table II shows that although other techniques require more than four logical operations, the suggested algorithm simply requires OR and XOR. Furthermore, the suggested technique requires a significantly smaller amount of hardware complexity than

others. Devices like Application-Specific Integrated Circuits, Logic Devices, and Programmable Gate Arrays are examples of hardware complexity.

Result

The hashed file is kept in a hashed format and is also known as a signed file. The "signature version" appears on the screen during execution, and then the user is prompted to provide the file name. The application then opens the file in read-binary (Rb) mode after asking the user for the file path. The hashing algorithm is next called, and after that comes the encoding function, which creates a unique code for every file by converting the hashed output into hexadecimal format.

VIII.CONCLUSION

This highly scalable and intuitive network security solution has been painstakingly designed to satisfy all suggested needs. Thorough testing has been done on all criteria, and almost all system objectives have been met with success. This technique offers considerable improvements over current approaches by eliminating human error and mitigating difficulties inherent in manual systems.

The software operates without a hitch, accomplishing the project's goals, and it may be extended even farther with small tweaks. Several platforms, such as digital electrical circuitry, computer hardware, firmware, software, or combinations of these, can be used to implement this concept. The apparatus may take the form of a computer program product that is meant to be executed by a programmable processor and is kept in a machine-readable storage medium. A programmable processor that is given instructions to operate on input data and produce output can carry out the method stages.

Furthermore, digital signatures strive for attributes like validity and verifiability that are seen in handwritten signatures. A subliminal channel's bandwidth measures its ability to communicate hidden information by determining how many covert messages it can send in a single protocol run. For messages under 1600 bytes, testing of new algorithms has shown a 4% reduction in the hashed file size relative to the original file.

IX.FUTURE ENCHANCEMENT

Future improvements can be applied to a variety of platforms, such as computer hardware, software, firmware, and digital electrical circuits, or combinations of these. The invention's apparatus can be implemented as a computer program product that is machine-readable and stored in a storage medium that a programmable processor can read and execute. The invention's method steps can be implemented by a programmable processor that runs an instruction program, allowing functions to be performed by processing input data and producing output.

REFERENCES

1. *R. Dharmarajan and V. Thiagarasu, " Network Security and Intrusion Detection System Using Data Mining Techniques", Proceedings of Asian Journal of Computer Science and Technology ISSN: 2249-0701 Vol.8 No.1, 2019, pp. 7-12.*
2. *Vikas Lokesh, Srivathsan Jayaraman, Dr. H S Guruprasad, " A SURVEY ON ETWORK SECURITY AND CRYPTOGRAPHY", Proceedings of International Journalof Advance research In Science And Engineering IJARSE, Vol. No.3, Issue No.10, October2014.*
3. *Amer Ibrahim',RaviSekhar".JamalFadhil Tawfeq',Sinan Q Sallh, Prltesh Shah', "Security and Privacy Protection for Online Electronic Documents Based on Novel Encryption Techniques ", Proceedings of Journal of lntlligent Systems andInternet of Thongs(JISloT) Vol.11,No.01, PP 21-28, 2024.*
4. *Abhishek Roy and Sunil Karforma, ""A survey on digital signatures and itsapplications", J. of Comp. and I.T. Vol. 3(1&2), 45-69 (2012).*
5. *Aradhana, Dr. S. M. Ghosh," Secure Hash Algorithm With Its Variants", Impact Factor:3.45 (SJIF-2015), e-ISSN: 2455-2584 Volume 3, Issue 05, May-2017*
6. *PATEL PRACHI PRAVINKUMAR," Secure Digital Signature Schemes based on HashFunctions", International Journal of Computer Engineering and Science, August- 2014.*
7. *Daniel Lloyd Calloway," Cryptography and its Role in Network Security Principles andPractice", Capella University, OM8302, § 4 8 September 2008.*
8. *Sur C., Roy A., Banik S., A Study of the State of E-Governance in India, Proceedings of National Conference on Computing and Systems 2010 (NACCS 2010), January 29, 2010,pp- (a)-(h), organized by : Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 8190-77417-4.*
9. *Roy A, Karforma S, Risk and Remedies of E-Governance Systems, Oriental Journal of Computer Science & Technology (OJCST), Vol: 04 No:02, Dec 2011 Pp- 329-339. ISSN 0974-6471.*
10. *Y. Wang, M. Martonosi, and L.-S. Peh, "Predicting link quality using supervised warning in wireless sensor networks," ACM SIGMOBILE Mobile Computing and Communications Review, Vol. 11, No. 3, pp. 71–83, 2007*
11. *Shouhuai Xu, Xiaohu Li, Timothy Paul Parker, Xueping Wang, "Exploiting Trust basedSocial Networks for Distributed Storage of Sensitive Data", IEEE Transactions on Information Forensics and Security, Volume 6, Issue 1, 2011, pp 39-52, DOI: 10.1109/TIFS.2010. 2093521.*
12. *Mohamed M.E.A Mahmoud, Xuemein (Sherman) Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on parallel and Distributed Systems, Volume 24, Issue 2, pp 209 - 229, 2013, DOI:10.1109/TPDS.2012.106.*
13. *D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen, "Untangling blockchain: A data processing view of blockchain systems," IEEE Transactions on Knowledge and Data Engineering, vol. PP, no. 99, pp. 1–1, 2018.*
14. *S. lnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," Government Information Quarterly, vol. 34, no. 3, pp. 355 –364, 2017.*
15. *M. D. Pierro, "What is the blockchain?" Computing in Science Engineering, vol. 19,no. 5, pp. 92–95, 2017.*
16. *N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1–1, 2016.*