Research Reports on Computer Science
https://ojs.wiserpub.com/index.php/RRCS/

UNIVERSAL WISER
PUBLISHER

Research Article in Special Issue: Selected Papers from the 4th International Conference on Machine Learning, Image Processing, Network Security and Data Sciences (MIND-2022)

# Securing Digital Information Using Cryptography Techniques to Enhance IT Security

**Swati Chaudhari[1*], Archana Thakur[2], Alpana Rajan[1]**

[1]Raja Ramanna Centre for Advanced Technology, Department of Atomic Energy, Govt. of India, Indore, M.P, India
[2]School of Computer Science & Information Technology, Devi Ahilya Vishwavidyalaya, Indore, M.P., India
E-mail: swati@rrcat.gov.in

**Received:** 8 March 2023; **Accepted:** 21 March 2023

**Abstract:** In information technology (IT) security, defence in depth is considered the best practice. Protecting data at rest or in transit is a part of the defence in depth approach. Confidentiality, data integrity, authentication, and non-repudiation are four IT security paradigms that need to be achieved to protect data and enhance IT security. Every scientific organisation requires i) to maintain the confidentiality of information like novel research ideas, results, patents, indigenous developed techniques and designs, human resource personal data and remarks, etc. ii) to manage the integrity of Internet-based web resources, users' credentials, etc. and iii) to manage non-repudiation and integrity guarantee enabled implementation of various software systems. The Rivest-Shamir-Adleman (RSA) technique is used to achieve confidentiality of secret data during its storage and transmission over insecure channels. The elliptic curve cryptography (ECC) technique is used for key exchange with extremely constrained devices like wireless and wireless sensor networks. Data hashing is used for maintaining data integrity; digital certificates are employed to achieve non-repudiation. In order to enhance IT security, the application of these cryptographic algorithms has been studied in data security like workflow-based applications, video conferencing, Domain Name System (DNS), web security, and radio frequency identification (RFID) systems and presented in the paper. A novel scheme to ensure website integrity and to detect website attacks using time-stamped hash functions with timestamping is also demonstrated in the paper. The study revealed that symmetric key and asymmetric key algorithms provide confidentiality and authentication. Data integrity and authentication are achieved using digital signatures and message authentication codes. Non-repudiation is established with asymmetric key algorithms and digital signatures.

***Keywords*:** data security, digital sign, hash, cryptography, workflow application security, DNS security, RFID security, video conferencing security

## 1. Introduction

After human resources, information is an organisation's most important asset. For secure systems and networks, it is desirable to achieve data availability, integrity, confidentiality, and non-repudiation; these are four paradigms of a secure system. No infrastructure security controls are 100% effective. Study and implementation of cryptographic

DOI: https://doi.org/10.37256/rrcs.2320232635

aspects play an important role in implementing data security.

## 1.1 *General overview of cryptography*

The term cryptography is a fundamental aspect of information security. People who develop algorithms to keep systems secure are called cryptographers. Cryptography takes plaintext as input, applies an encryption algorithm, and converts plaintext to cypher text, which is sent over an insecure channel to the receiver. The receiver then decrypts the cypher text using a decryption technique and gets back the plaintext. Modern cryptography can be broadly classified as:

**Symmetric key (secret key) cryptography**. In symmetric key cryptography, only a single secret key which is shared between the sender and the receiver is used for encryption and decryption.

**Asymmetric key (public key) cryptography**. In asymmetric key cryptography, a pair of keys is used; one key is used for encryption and the other for decryption. Plaintext is encrypted with the receiver's public key and can be decrypted by the receiver with its own private key.

**Cryptography hash functions**. Hash functions are used for one-way cryptography since plaintext cannot be recovered from the generated cypher text.

## 1.2 *Various security paradigms*

Different organisations, such as banking, corporate, military, and health sectors, store confidential information about research articles, patents, indigenous developed ideas, designs, human resource data, consumer/supplier/product data, financial status, and medical records. This data is processed and collected over the network and stored on computers in digital form. Threats to information come in many different forms, like software attacks, intellectual property and identity stealing, information sabotage, and information extortion. Hence, it is very important for any organisation to deploy information technology (IT) security mechanisms to protect against these attacks. The objectives of information security can be listed as:

- Confidentiality: Maintaining authorised restricted access to information reading, writing, and disclosure, containing methods for securing private and copyrighted information. Losing confidentiality means unauthorised leakage of information.
- Integrity: Protects against unauthorised information modification or destruction, including ensuring non-repudiation and authenticity. A loss of integrity is the unauthorised modification or destruction of information.
- Authentication: It verifies that the message being transmitted is by a legitimate and intended user only. Hence, it establishes trust and confidence that the system is receiving input from an authorised user.
- Non-repudiation: For secure message delivery, it ensures that the messages sent and received by the communicating parties have only sent and received the messages. Hence later, the communicating parties cannot deny about sending and receiving of the messages respectively.

The above-mentioned security goal(s) can be met by employing a variety of cryptographic techniques such as symmetric key, asymmetric key, and hash functions [1]. A general overview of various cryptography techniques is given in the next section.

## 1.3 *Various cryptography techniques*

**Symmetric key algorithms**. There are five components to a symmetric encryption scheme. (i) Plaintext: A message or data in clear text that is provided as an input to the algorithm. (ii) Encryption algorithm: Various substitutions and permutations are carried out by the encryption algorithm to convert plain text to cypher text. (iii) Secret key: The encryption algorithm takes the secret key as an input. The precise substitutions and permutations carried out depend on the key used, and also based on the particular key being used at the time, hence the algorithm will produce different outputs. (iv) Cypher text: As an output, a garbled message is produced based on plain text and the key. The cypher text is actually an unidentifiable random stream of data. (v) Decryption algorithm: It is basically running the encryption algorithm in reverse, forming the decryption algorithm. Original plain text is generated by taking cypher text and a secret key as inputs. Symmetric key cryptography has two basic requirements. (A) The assumption is that it is not possible to decrypt a message even if the cypher text and encryption/decryption algorithm are known. Hence, it is required that only the key be kept confidential. (B) Copies of the secret keys are to be communicated over a secure channel with the utmost security by two communicating parties, the sender and the receiver. If somebody gets the key and information about the algorithm, then all communication using the key is readable.

Encryption techniques have substitution and transposition as two basic building blocks. Substitution techniques: Plaintext's letters are replaced by numbers, symbols, or other letters. The plaintext bit pattern is replaced to obtain the cypher bit pattern by the substitution process. The Caesar Cipher, Polyalphabetic Ciphers, and Monoalphabetic Ciphers are variants of substitution techniques. Transposition techniques: Some sort of permutation is performed on the plaintext letters to achieve different kinds of mapping. Rail fence and rotor machine techniques are used in transposition techniques. Block cypher works on a group of bits which are called a "block". A block cypher is a symmetric key cypher which operates with constant transformation. A block cypher which takes in a 128-bit block of plain text generates its corresponding 128-bit cypher text. The transformation is guided by a secret key which constitutes the second input. Decryption is achieved by providing the decryption algorithm with the 128-bit block of cypher text and the secret key. The outcome is the original 128-bit block of plain text. Encryption of messages longer than the standard block size of 128-bit, can be achieved by the use of different modes of operation. Unlike block cyphers, stream cyphers work on individual bits which are taken one at a time. Hence, encryption and transformation operations differ in the case of stream cyphers.

Data Encryption Standard (DES) is an extremely powerful early cypher block. As academics critically examined it, motivation was created for a current understanding of block cyphers and their cryptanalysis. DES is not secure because of its small key size of 56 bits. It can be cracked within a few hours.

Some investigative studies revealed theoretical weaknesses in the cypher. The Triple DES form of the algorithm is considered to be practically secure. The cypher has been thrived by the Advanced Encryption Standard (AES) [1].

*DES*: DES is a substitution-permutation network (SPN) cypher suggested by Feistel. DES is now obsolete in which a 56-bit key was used, that can be cracked using brute-force methods. A 16-cycle Feistel system, in every cycle, the overall 56-bit key is permuted into 16 different 48-bit subkeys. For decryption, the matching algorithm is used with a reversed order of subkeys. The overall block size is 64-bit, containing 32 bits of L and R blocks each. A data block of 32-bit and one of the subkeys of 48-bit is taken as an input by the "f"-hash function specified by the standard using "S boxes" and produces a 32-bit output. 8 bits of the 64-bit key of DES are used for checking parity, so the actual size of the key is 65 bits [1].

*Triple DES*. Triple DES is a modified version of DES. The size of the key is increased by operating the algorithm thrice in sequence with three different keys. Applying three times 56-bit keys makes the key size 168 bits, which cannot be broken by brute-force techniques used by the Electronic Frontier Foundation (EFF) DES cracker machine. No serious design flaws could be discovered in triple DES, although initially the algorithm was considered as not so perfect. Today, in a number of Internet protocols, triple DES has been used in its cryptosystem [1].

*AES*. Rijindael combined the SPN model with field operations suggested by Galios in each round. The Galios field operations actually generate rubbish but can be precisely reversed, which is comparable to Rivest-Shamir-Adleman (RSA) modulo arithmetic operations.

**Asymmetric Key Cryptographic Algorithms**. These algorithms use a pair of keys, a public key and a private key. The public key is used for encryption while the private key is used for decryption. Some of them are discussed below:

*RSA*. Ron Rivest, Adi Shamir, Len Adleman conceptualized the RSA algorithm. It is the most popular and extensively applied general-purpose public key encryption algorithm. Block cyphers are made up of integers between 0 and n – 1 for n, where the size of n is mostly 1024 bits for plain text and cypher text. Cypher blocks of size of binary value less than number n are created after applying an algorithm to plain text. Calculating the hardness of RSA algorithms is an integer factorisation problem. Factorise a given number to calculate the prime factors, as it is a product of these two big prime numbers.

- RSA key generation: Consider 2 large prime numbers p and q with a given exponent value e which falls between 1 and ((p − 1)(q − 1)). ((p − 1)(q − 1)) and e cannot have a common factor except number 1. Actually, ((p − 1)(q − 1)) and e are coprime numbers. Public and private keys are generated with steps: (Step 1) n = p*q; (Step 2) e*d = 1 mod (p − 1)(q − 1); (Step 3) public key = pair of {n, e}; (Step 4) private key = pair of {n, d}
- RSA encryption and decryption: During encryption, a public key is applied to plain text m to generate cypher text c where c = me (mod n). During decryption, a private key is applied to cypher c to generate plain text where

m = cd (mod n). Decryption is equivalent to signature generation, and encryption is equivalent to signature verification [1].

*Elliptical curve cryptography (ECC) employs public key encryption*. It is based on elliptic curve theory, which is capable of creating smaller, more efficient, and faster cryptographic keys. Instead of using conventional methods of key generation like the product of very large prime numbers, ECC creates keys through the elliptic curve equation properties. As per the study carried out by researchers, ECC can achieve a level of security with a 164-bit key that other systems require a 1024-bit key to achieve. ECC has gained popularity because it provides equivalent security with low computing power and battery resources [2]. It is widely used for mobile applications.

*Digital Signature Algorithm (DSA)*. DSA is not an encryption algorithm and was developed only for signing data. A series of operations using selected prime numbers is performed during the signing process of DSA. Longer key sizes, even more than 1024-bit, are also supported by DSA. In the case of DSA, the process of generating a digital signature is faster than validating it, which is vice versa in the case of RSA [3].

Different cryptographic techniques are chosen depending upon the information security applications to achieve depending upon requirement of security paradigms. The rest of this paper is organized as follows. Section 2 discusses some major IT applications like workflow-based applications, video conferencing, Domain Name System (DNS), web security, and radio frequency identification (RFID) systems used in scientific organizations, their security requirements, and how cryptography techniques can be used to secure these applications. Section 3 presents practical aspects of how security is achieved using cryptography techniques and their implementation details. The outcome of the study is also presented in the form of results and analysis. Section 4 presents conclusions, future work and new trends in the direction of data security enhancement.

## 2. Scientific organisations' IT security requirements and major application areas

The primary goal of scientific organisations is to carry out premium-quality research in the field of science and technology. IT security requirements such as authentication, non-repudiation, confidentiality, data integrity, and availability of information have become important tasks. Every scientific organisation has precious resources like data, software, computers, etc. Authenticated access to these assets needs to be given to the members of the organisations only. Non-legitimate persons should not get access to the data, hence encryption of user passwords, human resources (HR) data, research results, designs, ideas related documents is required. Implementation of digital signatures, hash functions, and message authentication techniques of cryptography are widely used in such scenarios.

The goal of IT security in every organisation is to have policies for confidentiality of information like HR data such as appraisal letters, salary slips, emails, research results, ideas, and patents to protect it from theft, non-authorised modifications, and its secure transmission so that the legitimate user can only read it.

Nowadays, websites have become the face of any organisation, and hence they are a precious resource. Maintaining its integrity and protecting it from various attacks is an important task. An eavesdropper or intruder over a secure communication channel can tamper with the data. Results generated in the organisation are the fruits of the hard work of individuals. Therefore, important data (results) should not be altered or tampered with for the lifetime of data. In order to achieve data integrity, hash functions such as Secure Hash Algorithm (SHA)-2, Message Digest Algorithms (MD5) based checksum system, digital signature, and a message authentication technique of cryptography are implemented.

Non-repudiation in a scientific organisation refers to the fact that the owner of data cannot deny ownership. Non-repudiation in the case of email communication ensures that neither the email sender can deny having sent it nor the email receiver can deny having received it. Messages are transmitted among the parties by digital signatures to ensure non-repudiation.

### 2.1 *Public key infrastructure (PKI)/RSA for storing online secret data to achieve confidentiality*

A pair of two different keys known as a public key and a private key are used to carry out encryption and decryption. Communicating parties publish their public key in order to have secure communication in public key cryptography. To establish confidentiality between two communicating parties like A and B, Party A can encrypt a message using Party B's public key, which is available publicly. The communication would be decipherable only to

Party B, as the message could be decrypted by the corresponding private key, which is only known to Party B. Party A can encrypt the message using its own private key and send the authenticated message to Party B. This message is decryptable with Party A's public key only. This fact ensures the authenticity of the message by proving that the message was actually sent by Party A.

## 2.2 *ECC for wireless and wireless sensor networks*

A wireless sensor network is a collection of a large number of sensors used for a variety of applications like military surveillance, construction work safety, reactor safety, weather monitoring, etc. Due to their design (low cost and small size), they have limitations in memory and communication bandwidth. Each sensor that wants to communicate with another sensor has to send a key, which should be transmitted secretly over an insecure channel. If symmetric encryption is used, then there is a significant increase in key size. For the Diffie-Hellman algorithm with RSA to be secure, the key size should be 1024 bits. The same level of security can be provided by elliptical curve Diffie-Hellman key exchange with a key size of 160 bits. Thus, there is a significant decrease in key size with an increase in security [4]. In ECC, one of the most heavily used operations is scalar multiplication. 85% of the computation time is spent on this operation. Thus, some mechanisms can be employed to decrease the cost of scalar multiplication [1].

## 2.3 *MD5/SHA-1/SHA-256 hash functions for the intrusion detection system for monitoring and maintaining the integrity of an organisation's web-based resources deployed over an insecure network, as well as password storage*

MD5 and SHA are used for ensuring data integrity. A message of arbitrary length is converted to a 128-bit "message digest". It compresses a large file in a secure way and is hence used for digital signatures, which need to be compressed before being encrypted. However, MD5 has been proven to be "cryptographically broken and unsuitable for further use" in 2010. So, new SHA-1 and SHA-2 algorithms resembling MD5 came into existence. The current versions used for IDS (Intrusion Detection System) are SHA-256 and SHA-512, which use 32-bit and 64-bit words, respectively. A cryptographic hash function is computationally infeasible because it is extremely difficult to reconstruct the original data from the hash value. A change in any bit of the data block results in a change to the hash code. An IDS tries to detect and alert on attempted intrusions by observing suspicious activities during or before an attack. Network-based intrusion detection systems (IDS) can be used to gain access to network traffic by connecting to a network hub, switch, or tap to maintain network integrity over insecure networks. These systems first calculate the hash values, thereafter performing signature matching with the client and then implementing automata for the filtered signatures for reduction of false positives and negative alarms. The security of the network system can be enhanced with the use of encryption algorithms before the IDS. The second type of IDS is host-based IDS, which uses a database of system objects it should monitor. For communication authentication, the server and the client exchange a passphrase (a longer form of a password to improve security) that identifies them. This passphrase is stored and used for the entire session to create objects. The IDS remembers the elements of each object and uses the above-mentioned hash algorithms to create the checksum for the contents. This is stored in the secure database of Host Intrusion Detection System (HIDS) for later use, particularly during comparison to check integrity [1].

## 2.4 *A digital certificate for workflow-based applications to achieve non-repudiation*

Digital certificates are digital documents that use PKI technology to bind a public key to an individual's identity. These verify the claim that the particular public key belongs to a particular person or entity. The private key is stored at the user's place. Workflow management systems support the definition and execution of business processes. Applications based on these systems are flexible, reusable, and scalable in the changing model of business processes. According to the Workflow Management Coalition's (WfMC), non-repudiation is a very serious existing security concern in workflow applications because of inadequate audit and verification. At the time of dispute, senders and receivers may not trust each other's arbitration. A digital signature is used to ensure non-repudiation in the case of the above situation. But if the signatures are not provided by any authorised third party, they are trustworthy. So, a certificate issued by a certification authority that acts as a trust centre in the global web environment allows secure execution of workflow-based applications.

## 2.5 *Secure video conferencing using cryptography techniques*

AES is one of the best algorithms because of its high level of security and lower complexity, but it is costly. These conventional approaches are not adaptable to newly discovered peculiar security requirements. Also, these are not well suited for video encryption as they cannot process massive volumes of video data in real-time. According to recent surveys on cryptographic discussions, AES can be combined with other algorithms like chaos cipher to make it cost-effective [1]. Below are the few research papers where authors have given new cryptographic algorithms which have paved a secure path towards the security of video conferencing: A dynamic symmetric key encryption algorithm has been proposed for multicast and broadcast streaming applications in which the key is only known to the sender and the user and is distributed over transmission control protocol (TCP). Because of the random behaviour of integer factorisation, it is almost impossible to get the key using brute force or cryptanalysis. Considering the difficulties in calculating different block size of each video frame, it is very difficult for the attacker to achieve the transmitted video [5]. Recently, in 2014, a selective video encryption technique has been developed that needs less time but at the same time ensures security too. This technique encrypts different levels/layers of selective parts of video streams, which are divided into different frames like I-frame, P-frame, and B-frame. Since P-frame and B-frame are useless without I-frame, only I-frame is encrypted. Generally, selective video encryption is more complex than the naive algorithm, but the proposed algorithm in this paper claims to be faster, more compact, and independent of key sharing factor. Cryptographic techniques integrate video conferencing techniques with authentication by generating the identifiers at the packet level, thereby preventing impersonation attacks [6]. For audio-video communication, a web-based secure surveillance system can be developed which can use the existing intranet. This type of system can provide good quality services and centralised control over the users [7].

## 2.6 *Secure video conferencing using cryptography techniques*

Despite being a critical operational part of the Internet infrastructure, the basic DNS doesn't have any strong security mechanisms for data authentication or data integrity. Weak authentication makes it possible for an attacker to act as a legitimate DNS server and can insert a malicious record into the DNS database. Cryptographic digital signatures address security issues such as authentication by combining cryptographic (primarily public key cryptography) and digital signature features. Also, it is simple and easy to verify the digital signatures of somebody having the public key. DNS can also be configured with a cryptographic hash algorithm using a private security key for secure DNS and Dynamic Host Configuration Protocol (DHCP) updates [4]. Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) standards to provide origin authority, data integrity, and authenticated denial of existence to clients. Many techniques for implementing them have been proposed over DNSSEC. A few cryptographic DNS signature techniques can be given as:

- Securing DNS with ECC: The main advantage of ECC is having a smaller key size but the same level of security as in RSA. A smaller key size makes the computation faster, resulting in higher efficiency. Because of the scalar multiplication concept, this algorithm also saves memory and energy, which makes it more suitable for low-power applications as well. DNSCurve is a proposed DNS protocol that uses ECC.
- DNSCrypt: This is a documented protocol using highly secure, non-(National Institute of Standards and Technology, NIST) cryptography. It authenticates communication between a DNS client and DNS resolver by using cryptographic signatures to verify that resources originate from the chosen DNS resolver and have not been tampered with. It prevents spoofing but it does not prevent "DNS leaks".
- SK-DNSSEC and PK-DNSSEC: According to [4], PK-DNSSEC can be used to protect root and top level domains of a DNS tree while SK-DNSSEC can take care of the rest. These protocols plans, if properly implemented, offer a high level of security while reducing the network traffic and storage requirements. It also enables efficient mutual authentication [4].

### 2.7 *Cryptography in RFID application*

RFID technology is used in many application areas. Some of the application areas are access control, identification, vehicle tracking, inventory, payment systems, etc. If appropriate cryptographic mechanisms are not applied, then the privacy of the users carrying tagged items is potentially compromised. RFID-based identification requires authentication as a cryptographic service. To secure these applications and reduce the threats, implementation of AES on RFID tags, public-key cryptography, and ECC are used.

## 3. Case study implementation, results and analysis

Dealing with website hacking due to zero-day vulnerability [8] is a challenging task, and there is no foolproof security mechanism available for it. A case study to ensure website integrity and to detect website intrusion using a digitally signed, timestamped hash function has been done, and implementation has been carried out to give proof of concept. Defacement of a website is normally detected by users of the website. Immediate blocking of the defaced website becomes critical to stop further access and minimise damage to the reputation of the organisation. An innovative use of a one-way hashing function to detect web intrusion is presented here. The web browser plugin can be used to check website defacement and the generation of defaced pages using the checksum is being researched [9]. It is not feasible to have a checksum of every web page on all websites using a trustworthy separate party. Work related to website integrity is satisfied by computing the SHA-1 value of the web page and pushing it into the page [10]. Whenever a page is retrieved by a user, a hash is generated and compared with the pushed one. But this does not provide authentication as the hash is not digitally signed. The web page digest is used by many mechanisms [5, 11, 12] for detecting website intrusion and original contents can also be regenerated. However, if the web server itself is compromised, recovery is impossible and manual intervention is required.

The novel approach based on digitally signed timestamped hash value to detect website intrusion as early as possible and stop the website's access immediately is found to be feasible and effective. As shown in Figure 1, there are three components to the approach. (i) A web server hosting a website in the De-Militated Zone (DMZ) behind a firewall. (ii) A firewall server providing restricted and controlled access to the web server. (iii) An intranet-hosted security checking server that interacts secretly with the web server and firewall server.

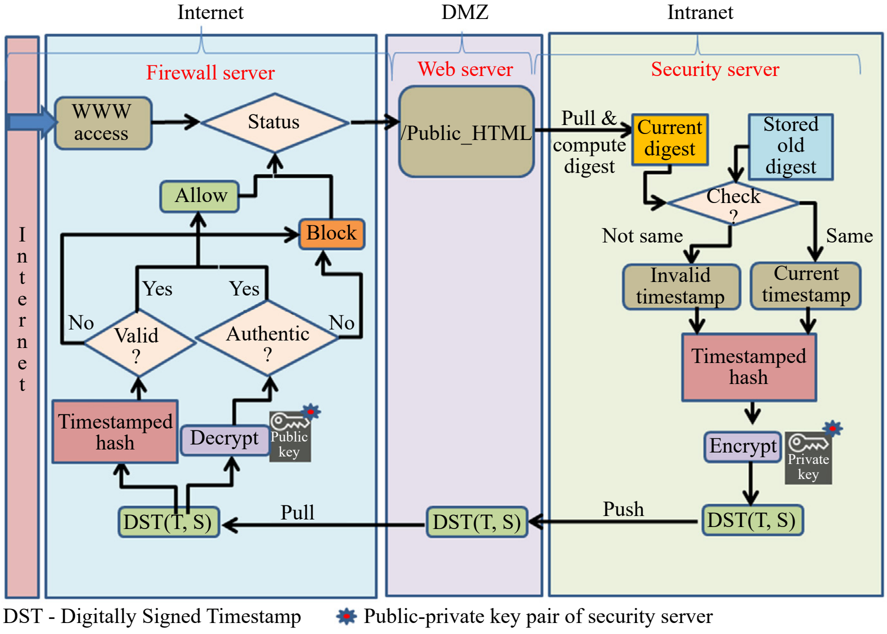

**Figure 1.** Workflow of the digitally signed timestamped hash value based implementation to detect website intrusion

The workflow shown in Figure 1 is explained as follows: The security checking server checks the integrity of the website at regular intervals and updates its validity. The firewall server checks the validity of the website at regular intervals and blocks it if its validity expires. The security checking server maintains a copy of the message digest of the website's public HyperText Markup Language (HTML) files. To perform an integrity check on a website, it executes a remote command on the web server to compute the current digest and compare it with the stored one. If both message digest values are the same, then only the security checking server updates the validity of the website, otherwise, it expires the validity. For updating/increasing the validity of a website, a security checking server digitally signs the current timestamp with its private key and puts it on the web server. This timestamp is valid for a specific duration in seconds. The firewall server downloads the digitally signed timestamp and verifies it with the help of the security checking server's public key. It also checks that the timestamp is valid, that is, not older than a specific duration from the current time. The advantage of using a signed timestamp is that if a web server gets compromised and an attacker stops the checking process by restricting the security checking server, the validity expires automatically and the website will get blocked within a few seconds. It prevents website users from getting fake information and stops any further adverse implications.

Web pages are updated on web servers through a security checker server. The server maintains a set of website files and their hash digest value as per the current files as and when the site is updated by the website manager.

The website validity timestamp is updated on the web server at regular and frequent intervals remotely from the security checking server. The security checking server for updating the validity timestamp; remotely computing the message digest of web pages kept in the public HTML directory of the website recursively on the web server. Then, it compares it with the previously stored message digest value. If both hash values are the same, then it digitally signs the current timestamp and copies the digitally signed timestamp to the web server. If not, it digitally signs an invalid timestamp and copies the signed invalid timestamp to the web server. In the case of a website attack, a security checking server can detect the exact web pages that have been added, modified, or deleted by the intruder. The security checking server detects a modified list of web pages by comparing it with the previously stored list. After detection, it can be immediately notified to the website administrator through an alert notification system for immediate attack mitigation actions.

In the event of an intrusion, the firewall server restricts ports such as 80 and 443 as the firewall server only forwards client requests for a web page to the web server. Blocking and unblocking of these requests can be controlled at the firewall server with the help of disabling and enabling World Wide Web (WWW) access requests by port forwarding for the web server. The firewall server is used for blocking and unblocking website access. It downloads the digitally signed timestamp from the web server at a fixed time interval. Check the authenticity and validity of the timestamp. Authenticity is verified by the public key of the security checker server. A timestamp is said to be valid only if it is not less than the specified duration, say in seconds, from the current timestamp. If the timestamp is authentic and valid, then website access is enabled, else it is disabled by manipulating port forwarding. This is implemented using bash shell scripts on the firewall server and executed on hardened OpenBSD servers. In our implementation, it takes a few seconds to block the website in the event of an intrusion. Our measured time is within 20 seconds. A Network Time Protocol (NTP) server [13] is used to synchronise the clocks of all servers. GnuPG [14, 15] is used for creating signed timestamps. For implementation, an OpenBSD based Packet Filter firewall [16] is configured.

Many types of software systems use cryptographic technique(s) for required functionalities or operations. Message authentication codes, public key authentication techniques, and other methods can be used for authentication. The authorisation can be accomplished through the use of an access control list. Confidentiality can be achieved by encryption and decryption. Data integrity can be achieved using various hashing techniques such as MD5, SHA-1, SHA-2, and so on. Non-repudiation can be achieved by digital signature. Table 1 lists different security services with different cryptographic techniques.

**Table 1.** Comparison of different IT security services with different cryptographic techniques

| Services | Symmetric key algorithm | Asymmetric key algorithm | Digital signature | Message authentication code |
|---|---|---|---|---|
| Message confidentiality | Applicable | Applicable | None | None |
| Message integrity | None | None | Applicable | Applicable |
| Message authentication | Applicable | Applicable | Applicable | Applicable |
| Message non-repudiation | None | Applicable | Applicable | None |

To achieve confidentiality of online secret data, the RSA algorithm of PKI is used for storage. Due to limitations of memory and communication bandwidth, ECC algorithms are more suitable and very effective for key exchange among the communicating sensors in wireless and wireless sensor networks. Websites are always at risk as they are deployed over the Internet. Innovatively, an intrusion detection system can be built to monitor and maintain its integrity of it using hash functions. Various hash functions are used to store passwords as well. Non-repudiation is established for the secure execution of workflow-based applications using digital signatures. Various customised cryptography algorithms can be used for securing video conferencing traffic, DNS records, and RFID applications.

## 4. Conclusions and future work

This paper presents a brief study of areas of applications where cryptographic algorithms can be used. The use of the Internet and networks is growing rapidly. Protecting data handled by network services is an important component of a defence in depth approach. Inevitably, there is a need to protect the data communicated over insecure networks by network services and applications. Various encryption techniques are applied to secure data in transit and at rest. An investigative study was carried out into the various application areas of cryptographic techniques and presented in the paper. A symmetric key and an asymmetric key algorithm provide confidentiality and authentication. Data integrity and authentication are achieved using digital signatures and message authentication codes. Non-repudiation is established with asymmetric key algorithms and digital signatures.

Data at rest or in transit is secured using various cryptographic techniques. For secure communication, basically, it is required to create a cryptographic system along with secure keys. Encrypted and authenticated messages are communicated between the client and the server using cryptographic techniques. Data transfer occurs after appropriate agreement between communicating nodes. The RSA technique is used to achieve confidentiality of secret data storage and transmission over insecure channels. The ECC technique is used for key exchange with extremely constrained devices like wireless and wireless sensor networks. Data hashing is used for maintaining data integrity; digital certificates are employed to achieve non-repudiation. Video conferencing, DNS security, and RFID systems are also prominent application areas. We demonstrated a novel approach to maintaining website integrity, managing intrusion detection, and preventing website access in the event of an attack by utilising cryptographic techniques such as message digests and digitally signed timestamped hash digests.

More secure than passwords and one-time passwords (OTPs), Fast Identity Online (FIDO) authentication techniques will be explored in the future. A study towards making use of personal attributes for encryption and decryption will be carried out. The current cryptography techniques must be able to face new challenges like smart attacks, quantum computing power, etc. New trends are to be adopted in data security practices. The evolution of new quantum-resistant cryptographic algorithms will be needed in the future. To increase data protection, bringing your own encryption model (BYOE), which does not require a PKI management party, is under discussion. Recently, blockchain is being used for data security in which the data is encrypted, distributed on a network and cross-checked by multiple nodes. Homomorphic encryption is a new trend that needs to be explored.

## Conflict of interest

The authors declare that there is no conflict of interest.

## References

[1] Stallings W. *Cryptography and network security*. 5th ed. Boston: Pearson; 2011.

[2] Froehlich A. *What is elliptical curve cryptography (ECC)?* http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography [Accessed 10th March 2022].

[3] Wikipedia. *Digital Signature Algorithm*. https://en.wikipedia.org/wiki/Digital_Signature_Algorithm [Accessed 10th March 2022].

[4] Tiwari NK, Khakhil S. Security system for DNS using cryptography. *International Journal of Computer Applications*. 2015; 120(17): 12-15. https://doi.org/10.5120/21318-4323

[5] Masango M, Mouton F, Antony P, Mangoale B. Web defacement and intrusion monitoring tool: WDIMT. In: *2017 International Conference on Cyberworlds (CW)*. Chester, UK: IEEE; 2017. p.72-79. https://doi.org/10.1109/CW.2017.55

[6] Down PH. *Introduction to Video Conferencing System*. http://www.video.ja.net/intro/#top [Accessed 10th March 2022].

[7] Singh G. *Secure Video Conferencing for Web Based Security Surveillance System*. Master's thesis. Indian Institute of Technology Kanpur; 2006.

[8] Stouffer C. *What is a zero-day exploit?* https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html [Accessed 20th February 2022].

[9] Kanti T, Richariya V, Richariya V. Implementing a web browser with web defacement detection techniques. *World of Computer Science and Information Technology Journal*. 2011; 1(7): 307-310. https://www.academia.edu/download/30987268/Implementing_a_Web_Browser_with_Web_Defacement_Detection_Techniques_.pdf

[10] Li B, Li W, Chen YY, Jiang DD, Cui YZ. HTML integrity authentication based on fragile digital watermarking. In: *2009 IEEE International Conference on Granular Computing*. Nanchang, China: IEEE; 2009. p.322-325. https://doi.org/10.1109/GRC.2009.5255107

[11] Masango M, Mouton F, Antony P, Mangoale B. An approach for detecting web defacement with self-healing capabilities. In: Gavrilova M, Tan C, Sourin A. (eds.) *Transactions on Computational Science XXXII*. Lecture Notes in Computer Science, vol 10830. Berlin: Springer; 2018. p.29-42. https://doi.org/10.1007/978-3-662-56672-5_3

[12] Huang Y, Sood A, Bhaskar RK. Countering web defacing attacks with system self-cleansing. In: *Proceedings of 7th Word Multiconference on Systemics, Cybernetics and Informatics*. Orlando, Florida, USA: International Institute of Informatics and Systemics; 2003. p.12-16. https://cs.gmu.edu/~asood/scit/defacing.pdf

[13] Lavigne D. *Network Time Foundation's NTP Support Wiki*. https://support.ntp.org/ [Accessed 20th February 2022].

[14] The GnuPG Project. *The GNU Privacy Guard*. https://gnupg.org/index.html [Accessed 20th February 2022].

[15] The GnuPG Project. *The GNU Privacy Guard Manual*. [PDF] 2022. https://gnupg.org/documentation/manuals/gnupg.pdf [Accessed 20th February 2022].

[16] OpenBSD. *OpenBSD PF – User's Guide*. https://www.openbsd.org/faq/pf/ [Accessed 20th February 2022].