Engineering and Technology Journal e-ISSN: 2456-3358
Volume 08 Issue 08 August -2023, Page No.- 2665-2678
DOI: 10.47191/etj/v8i8.24, I.F. – 7.136

Enhancing Data Privacy in Government Organizations: A Comparative Analysis and Implementation of Optimal Certificateless Schemes

Gabriel Kofi Armah[1], Hayford Ntiamoah Ofosu[2], Valentine Aveyom[3]
[1]Business Computing Department, School of Computing and Information Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana.
[2]Computer Science Department, College of Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
[3]Department of Computer Science, School of Computing and Information Sciences, C. K. Tedam University of Technology and Applied Sciences, Navrongo, Ghana.

ABSTRACT: The rapid expansion in Technology has transformed our everyday objects into interconnected entities, globally changing connectivity through the Internet and reshaping human interactions with their surroundings. This paradigm shift has occasioned the need for various networked infrastructures to facilitate and improve innovative services as well as enhance the flexibility and efficiency in this human- environment interactivity. However, this digitalization drive has also brought forth a range of security concerns that cannot be neglected.

This paper emphasizes on the role of certificateless systems in addressing security challenges posed by the digital realm on government organizations based on four fundamental security measures. These measures include confidentiality, integrity, authentication, and non-repudiation. The paper aimed at safeguarding data from unauthorized access, ensuring data integrity during transit, validating user identity and providing data integrity.

To enhance these security aspects, the study advocates the adoption of certificateless encryption techniques to uphold data confidentiality and employs digital signature techniques to guarantee integrity, accuracy, and non-repudiation. And the assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity. The study's main achievement a comparative analysis of four certificateless schemes to ensure data privacy from malicious attacks, Implementation of the best scheme using an elliptic curve digital signature and data-at-rest encryption. This ensured secure data privacy in transit and at retention to enhance confidentiality, integrity, and authenticity.

KEYWORDS: Privacy**,** non-repudiation, authenticity, encryption, comparative implementation, confidentiality.

INTRODUCTION

Technology is expanding field that offers a global connection to the Internet by turning everyday objects into interconnected ones due to digitization and altering how people interact with the things around them. This has led to a variant way for the development of networked infrastructure, cloud computing, and the internet of things to support creative services that guarantee more flexibility and efficiency. Such advantages are appealing to user applications and the industrial sector. However, despite their convenience and usefulness, there had been some cyber threats to individuals, government organizations, and firms invading their privacy such as identity theft, phishing, ransomware for their gain, and denial of services.

Organizations have been impacted by increased digitalization since it has made it possible for businesses to collaborate in new ways, resulting in new product and service offerings and new ways for an organization to interact with its clients, workers, and partners. At the same time, this digitization has put pressure on organizations to ensure data privacy. The need for data privacy has necessitated the adoption of various cryptographic technologies such as the use of certificateless schemes and digital signatures. A class of cryptographic techniques known as authenticated encryption guarantees both message secrecy and authenticity. It is a crucial element of practically all widely used cryptographic protocols.

Cryptosystems are designed to send and receive messages securely without the necessity of two shared secret keys. There are two approaches to cryptographic systems: Symmetric and Asymmetric. A symmetric key, also known as a secret key, employs a single key to both encrypt and decrypt the data. Smaller data collections and one-to-one sharing are where this works best. One private key and one public key are coupled in asymmetric or public key cryptography. Anyone can use the encryption key as it is made public. The reverse key, which is kept secret, is used to decode. Using a public key that has been approved by public key infrastructure, the sender encrypts a message using public-key encryption. The recipient's public key and digital identification are connected by the certificate. The adoption

is to guarantee that private information is never exposed, regardless of the transmission method, ensuring privacy.

MOTIVATION AND CONTRIBUTION

Though organizations have deployed various methods and techniques of security mechanisms to ensure data privacy, a significant portion of data breaches is caused by the negligent or unintended leaking of sensitive information. Most end-users are unfamiliar with security awareness and security processes, and employees routinely share and permit access to valuable data. However, most organizations and end-users of a system do not prioritize security which leads malicious persons to leverage it to leak sensitive data and cause damage to the organization's information technology infrastructure. This paper will evaluate four cryptographic schemes, and present a comparative analysis of their strengths, weaknesses, and methods to adopt the finest scheme to implement to ensure data privacy. Moreover, encrypting, and decrypting messages in transit and at retention using an effective cryptographic algorithm ensures the confidentiality, integrity, and authenticity of data privacy is ensured.

This paper's contribution is to facilitate a cryptographic algorithm scheme (Elliptic curve digital signature algorithms) to ensure data privacy, encrypting the data seamlessly with two-generation keys, a private key, and a public- key using a combination of Elliptic curve digital signature algorithms (ECDSA) and Data at-rest encryption (DARE) for implementation, which ensures that precise defensive measures are engaged when data changes states, guarantee that data is always secure. When communicating sensitive, private, or secret information over the internet, data encryption is a crucial privacy tool. Even if hackers, fraudsters, and other internet snoops manage to intercept plain text before it reaches its intended receivers, encryption scrambles it into a form of secret code that they are unable to decipher. When the communication does reach its intended audience, they may decode it using their key to restore the content to plain, readable language. Therefore, data encryption can aid in securing the data used to communicate, receive, and save on a device. That may consist of email messages, organization contracts on the laptop, health records kept on cloud infrastructure, and financial data supplied through your online account. In the process of data encryption, ordinary text, such as a text message or email, is shielded into "cipher text," which is an unintelligible format. This aids in preserving the privacy of digital data that is either transported across a network like the Internet or saved on computer systems.

RELATED WORKS

One of the workable approaches to ensuring data integrity and identity authentication for applications and devices is a certificateless signature. Certificateless signature does away with the complex certificate management and key escrow. Many certificateless signature techniques have been proposed recently, however, only a small number of them are secure and appropriate for data privacy and the internet of things.

Tajammul, Parveen, and Tayubi, 2021; In their research, proposed different security techniques that are used in cloud computing to protect data kept on cloud storage were compared and analyzed. Various security attacks, security objectives, and security-related topics have been covered in their work. They also addressed how to analyze and select from a variety of accessible algorithms in their research. In order to safeguard the data, for instance, some portions of the document should be encrypted using one technique while the remainder must be encrypted using another. However, their research path did not apply any of the algorithms in combination.

Makarenko et al., 2020, evaluated various symmetric block-based cryptographic algorithms and compare them to comment on their features, which will help in choosing the best method for a certain application. Energy, memory, and throughput are taken into consideration while comparing the algorithms. The comparison is carried out using z1 motes in the Cooja simulator, and the source code is available in the GitHub repository. The research undertook an exploratory investigation on the cryptographic algorithms used in IoT communication based on market trends, popularity, and fairness of the comparison. It evaluated the performance and applicability of the chosen cryptographic algorithms for resource constrained IoT devices. It also examined and used 11 alternative IoT encryption algorithms in the article, varying the block size, key size, and the number of rounds while considering prior research. After that, a comparative analysis of the chosen algorithms, rating them according to the following standards: throughput, power, energy, and memory consumption.

Li, 2022, primarily examine the many sorts of algorithms, choosing appropriate typical algorithms for each type, summarizing their working principle, comparing, and contrasting their benefits and drawbacks in terms of security and execution speed. It describes the underlying logic behind the chosen common algorithms. The research contrasted the variations in security, execution speed, and other factors, examining the benefits and drawbacks of each in real-world applications. It also introduced three different categories of algorithms: message digest algorithms, symmetric-key encryption techniques, and asymmetric-key encryption algorithms but couldn't predict bio cryptography. Gautam, Gaur and Masood, 2019, The research is concerned with the security techniques used in wireless sensor networks transferring sensitive data over the nodes deployed in a hostile environment. Discussion and comparison have developed throughout the paper, and a proposed approach based on the Elliptic curve digital signature algorithm

(ECDSA) as Elliptic curve-based certificateless signature for identity-baes encryption (ECCSI) algorithm as a result will reduce the energy cost in communication from the base stations and secure both the receiving end and the sender side by using a certificate-less approach.

ORGANIZATION

The rest of this study is organized as follows. Introduction, contextual information, motivation and contribution, and related works are all included in section 1. The breakdown of cryptography, encryption, the need for data privacy, and privacy attack vectors can be found in Section 2. The design model, comparison analysis, and implementation of best scheme covered in Section 3. Section 4 result and discussion, and Section is the conclusion.

BACKGROUND

Using the digital certificate from the public key infrastructure, which generate cryptographic scheme which ensure data privacy is achieved by encoding and encryption, this provides high security to systems, end-users, and application services such as web services and portals using the right algorithms. The importance of protecting data privacy is emphasized in this chapter, which will discuss cryptography, encryption, attacks, certificateless systems, and digital signatures, to maintain data privacy, compare four certificateless systems and adopt the best one.

CRYPTOGRAPHY

Advanced mathematical concepts and formulae are needed to store, transmit, and decode codes. The cryptographic key is used in this situation. An encryption key: a string of characters and numbers that are used to jumble data so that it seems random and unintelligible. Frequently, keys are brief enough to be remembered.

Takes on Encryption

Cryptography and encryption are interrelated but distinct ide as. Encryption is a cryptographic technique, which means th at it involves the computational complexity steps involved in producing and deciphering an encoded message. Users oug ht to ensure their data is secure because so many gadgets no w favor cloud storage. This assurance can be provided throu gh strong encryption.

Why Encryption functions

The cryptographic key makes up the mathematical equation of encryption. In addition, plaintext, ciphertext, and encryption techniques are considered. The collection of encryption algorithms is what implements encryption. Also known as ciphers, algorithms are mathematical formulas. An encoded message can be sent in ciphertext, which is unintelligible. The message or answer to the mathematical problem is in plaintext once it has been decrypted. The plaintext signal is initially scrambled by the method such that it no longer resembles its ciphertext opponent during the encryption phase. When the ciphertext has to be decoded, a different method employs a key to unlock the ciphertext and restore the original plaintext of the communication. There might be one or two keys in use, based on the kind of encryption that is being utilized. Data Encryption Standard (DES) is an early and less secure type of encryption that is now seldom ever used to safeguard sensitive data. To further improve the encryption, the original DES algorithm is repeated three times which introduced Triple DES. It is most frequently used in financial industries and has three keys, each of which has 56 bits. The Advanced Encryption Standard, which uses keys of 128, 192, and 256 bits, is thought to be the safest algorithm type now. The U.S. government and several private sectors rely on AES as their trusted standard. RSA is also a strong, dependable, and widely used public-key encryption method for protecting data transferred over the internet.

Diagram of how encryption works

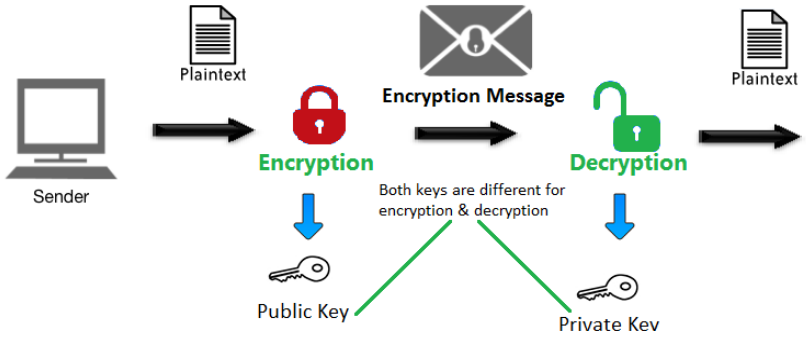

Figure 1: Diagram of how encryption works

FORMS OF ENCRYPTION

Asymmetric encryption sometimes referred to as public key encryption or cryptography encrypts and decrypts data using two separate keys. The message is converted from plaintext to ciphertext by using the public key to encrypt it. The private key converts ciphertext back to plaintext after decrypting it. Although each private key is unique to the receiver, the public key is accessible to everyone. Asymmetric encryption is

usually safer since it requires two distinct keys. This is so that the private key is required to decrypt the encoded message. It is a slower process, though.

Symmetric encryption on the other hand requires one private key for encryption and decryption of data. Symmetric encryption uses only one key, which makes it less secure than asymmetric encryption but faster to implement. Since there is only one secret key, another drawback is that all parties who want access to the plaintext message must share the key before decoding can take place. AES and Triple DES have taken the role of several antiquated symmetric encryption techniques like DES. Online payment systems and random number generation frequently employ this kind of encryption.

Pros of Encryption

Any sensitive data or intellectual property exchanged or kept online is safeguarded by file encryption. Although ransomware mostly targets businesses, people can also become victims. However, an additional layer of security like encryption might assuage your concerns.

Privacy

Encryption techniques provide you control over your data and prevent your sensitive information from falling into the wrong hands. Internet security is made possible by encryption when utilizing protocols like SSL and HTTPS. When submitting personal information to make purchases or sign up for communications, users may trust such websites. You can be confident that any personal information, signatures, or passwords are secure by encrypting emails. Limit the amount of information you post online and delete your digital footprint to further secure your privacy.

Why data privacy

A government data hack may also jeopardize the security of entire nations. Additionally, if it happens within your business, it may expose your confidential information to a competitor.

Cybersecurity threats are increasingly becoming a commonplace aspect of modern life. Due to the proliferation of smartphones, social media, dating apps, and online banking, internet-connected gadgets are more and more ingrained in our daily lives. As our relationships with our electronic gadgets deepen, so do the cybersecurity risks we face and the chances that third parties would use our data for their financial advantage. How we treat bits of information (referred to as "data") in terms of their suitability for secrecy is what is meant by the idea of data privacy. Data are not all made equal. For instance, you could feel at ease telling a total stranger your name. You're less likely to provide your home location though. There should be a need to establish guidelines and practices to protect the privacy of our sensitive personal data as a result. Critical information about a person's personal or professional life is referred to as data privacy. Due to its capacity to identify your identity in real life, this data is sometimes referred to as "personally identifiable information" (PII). Examples are Citizen Identification number, full name, etc. Data privacy is highly concerned with safeguarding private data connected to business activities daily. For instance, a private company will wish to safeguard any information related to its research and development contract, balance sheets, income statements, or the information of its clients. Sensitive information can be used by bad actors to extract cash or intellectual property from them. Additionally, there are several cases of cybercriminals and hackers using private information, such as bank account numbers or photos, as ransom. The answer is that businesses must go above and beyond to safeguard their users' and customers' data.

Data privacy attack

Insider threat attack

A security risk known as an insider threat comes from within the targeted organisation. It usually involves a current or former employee or business acquaintance who gains unauthorized access to private data or privileged accounts on an organization's network, they maintain access for malicious access for their gain.

SQL injection attack

By introducing special characters to a user input that alter the context of the query, SQL injection manipulates SQL code. The database anticipates processing a user input, but begins processing malicious code that serves the attacker's interests. SQL injection can disclose client information, proprietary information, grant attackers administrator access to a database, all of which can have dire repercussions.

Trading- attack

The third of the "top 3" privacy concerns, trading, is when thieves exchange the financial and personal information they took from your computer or from a computer belonging to a third party that housed your data. Visit chat forums where stolen identity data is sold to the highest bidder for between $1 and $3 for each name to see how common trading is, sadly. Once the information is sold, it can do irreparable harm to someone's life or financial reputation. Cybercriminals will register new credit card accounts, buy expensive electronics or goods, or engage in a range of other illegal activities using stolen or exchanged information.

Significance of data privacy

It is crucial to protect sensitive data and private information. Information about finances, health, and other private consumer or user data can put people in danger if it falls into the wrong hands. Individuals may be at risk for fraud and identity theft due to a lack of access control over personal information.

Certificateless signature schemes

Certificateless signature is a practical cryptographic tool that is used to provide data integrity and identity authentication in the web technology, network infrastructure, Internet of Things, eliminating the need for onerous certificate management in certificate-based signature systems and the key escrow issue in identity-based cryptosystems.

Certificateless encryption features:

- They provide security without requiring a digital certificate to verify a public key.
- They are impervious to outside attacks

You'll need two public-private key pairs for this: - A typical pair that the receiver produces. To prevent misunderstandings with the entire private key of the scheme, the value of the private key is referred to as a secret value. It's important to keep in mind that even though the public key value is well known, it cannot be verified using a digital certificate. a set of identity-based keys given by a key generation center that consists of the receiver's digital ID and the related identity-based private key. A "partial private key" is what this private key is called. Using the recipient's public key and digital identification, the sender encrypts the message. The partial private key provided by the key creation center and the secret value the receiver created are used to decipher the ciphertext. Because a message cannot be deciphered by an attacker who creates a false public key for an identity because the attacker lacks access to the whole private key for that identity, it is presumed that the sender does not need a digital certificate. Comparable to an identity-based encryption system is this way of thinking. The secrecy of a transmitted message cannot be compromised by the key generation center since it is unaware of the secret value that corresponds to the recipient's public key. This implies logically that a key generation center won't supply a recipient with a fake public key. In Public Key Infrastructure, the digital certificate that links the public key to the identification of a person or an organization identifies the owner of the key. The Certificate Authority, a Trusted Third Party in responsibility of issuing certificates, is the essential part of a PKI. Each digital certificate issued by various Certificate Authorities can be mutually recognized on a large-scale infrastructure to create a trusted environment. Public key infrastructures are constrained in their ability to expand due to the incompatibility of the digital certificates issued by various certificate authorities, which makes them an expensive technology to maintain. Shamir first unveiled the Identity-based Cryptosystem as an encryption method in 1984. In IBC, a user's public key is generated by using a public hash function on a user identifier that is accessible to the general public, such as an email address, username, or IP address.

Without exchanging public keys, this method enables two users to engage in secure communication and verify one other's signatures. After the user's identity has been confirmed, a reliable third party by the name of Private Key Generator can give them the relevant private key. This verification is comparable to what is needed to issue a certificate in a normal PKI.

Expatiating Public key infrastructure (PKI)

By enabling the interchange and verification of data across multiple servers and users, PKI enables secure connections between the server and the client.

PKI is based on digital certificates that are encrypted and decoded to confirm the legitimacy of the transaction by confirming the identity of the client, internet of things, and computer servers. In the modern digital era, when the number of devices is continually growing, our data must be reliable and impervious to attacks.

Digital certificate

Digital certificates are necessary for PKI operation. Digital certificates are a type of electronic identification. Since certificates can be used to confirm a party's identity, PKI enables safe connections between two communicating machines. By creating their own certificate through internal communications, a company can obtain these certificates from a trustworthy third-party issuer, which is the Certificate Authority.

Certificate Authority

Entities, such as users, computers, and servers, can validate their digital identities using a Certificate Authority. The certificate authorities, who also prohibit fraudulent businesses, are in charge of overseeing the life cycle of any particular number of digital certificates within the system.

Registration Authority

The Certificate Authority has authorized the Registration Authority to issue digital certificates to users on a case-by-case basis. Every certificate that the Registration Authority and the Certificate Authority seek, approve, and revoke is kept in an encrypted certificate database.

The certificate store, which is typically based on a particular computer and serves as a storage area for all memory pertinent to the certificate history, including issued certificates and private encryption keys, is another location where certificate history and information are kept.

The significance of public key infrastructure

Digital certificates serve as a "digital footprint" of the parties' identities and honesty. They aid in proving that a specific public key belonged to a specific entity.

Public key infrastructure can be used for the following to protect sensitive data:

- Email security,
- Web security – securing website SSL certificate
- Application security – signing applications
- Chipset smart card authentication

A COMPARATIVE ANALYSIS OF THE BEST CERTIFICATE LESS SCHEME IS IMPLEMENTED TO ENSURE DATA SECURITY.

A succinct explanation of digital signature.

A mathematical method known as a digital signature proves the validity of digital messages or documents. The file or message being sent has a private key signature. The recipient's message is verified using their public key. Digital signature aid you to sign documents, utilizing a public and private key that only you have access to, to encrypt the document. The legitimacy of that document is ensured by that private key. The digital signature certificate is employed for both encrypting and signing. It is practical for users who need to authenticate and uphold the privacy of shared information. It is used for submitting applications and documents to the authorities. In **fig.2** As soon as a document is uploaded for signing, a cryptographic hash is created for it. This hash is then encrypted using the sender's private key, store in a secure hardware security module box, and is then added to the document and delivered to the recipients together with the sender's public key. The signed data is hashed, and if the results match, the signature is validated. The signature is decrypted using the public key to obtain the original hash value.

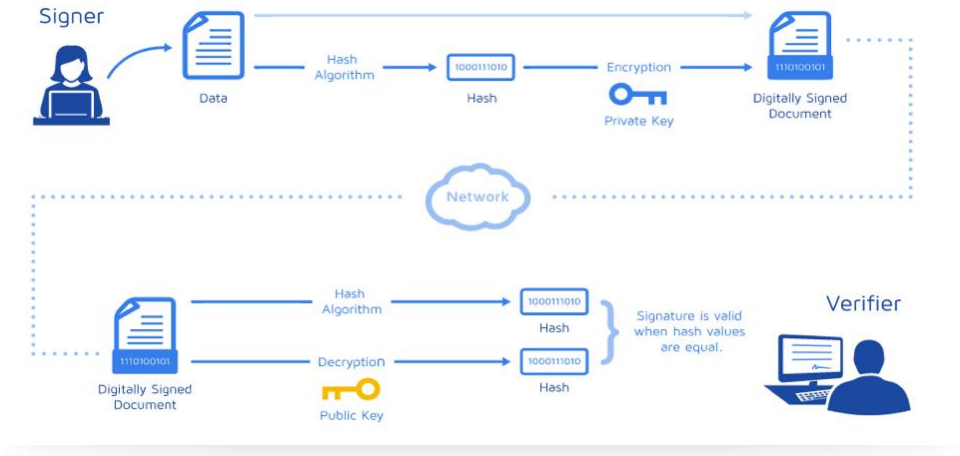

Figure 2 the process of digital signature

Differentiate between an electronic and a digital signature

Table 1:

A digital signature	An electronic signature
Is a signature that offers cryptographic evidence of a document's integrity and authenticity, as well as the authenticity of the signer's signature. To authenticate a sequence of data and determine a signature's provenance and document authenticity, it employs a cryptographic procedure and an algorithm.	Utilizes electronic symbols connected to a record to confirm a signature's author. certifies a signer's intention to sign a document, whereas it does not show the signer's identity or the integrity of the document.

Table. 2 Distinguish between digital signature and electronic signature

Comparative analysis of the four certificateless schemes

Table2:

PAPERS	OBJECTIVES	STRENGTH	WEAKNESS	EFFICIENCY

(Yu et al., 2021) Yu, H. et al. (2021) 'Certificateless Signcryption Scheme from Lattice', IEEE Systems Journal, 15(2), pp. 2687–2695. doi: 10.1109/JSYST.2020.3007519.	objective is to establish certificateless signcryption scheme from lattice (L-CLSS) It simultaneously performs the dual tasks of certificateless signature and encryption.	It simplifies the management of certificates and reduce the extra computation cost. It can simultaneously fulfil public key encryption and digital signature operations in one logical step with a much lower computation and communication cost than signing-then-encrypting way. It resists quantum computing attacks. solves the issues with certificate administration and key escrow. Engineering can use an effective and secure L-CLSS scheme in many different ways.	Lattice-based signcryption is developing slowly.	L-CLSS has better computing efficiency and less communication overhead than previous schemes, analysis demonstrates that it is a great system.
'Certificateless Homomorphic Signature Scheme for Network Coding' (Chang et al., 2020)	a novel idea for network coding with homomorphic signatures without certificates	Compared to other efficient certificateless, homomorphic schemes, is the most efficient and secure hence appropriate for networking code.	Constraints of a random oracle	According to its performance analysis, the scheme is more efficient and secure than existing successful CLHS schemes, making it more appropriate for network coding.
'Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices.' (Shu et al., 2020)	It fixes the key-escrow problem that plagues contexts based on identity.	it has been shown to be secure and unforgeable.		The efficiency analysis shows that the computation costs of our PF-CLS scheme are less than those of existing certificateless based signature systems already in use, making the proposed system more efficient. devices with limited processing power, communication bandwidth, and storage that are appropriate for usage in areas with limited resources.

B, Z. C. and Chen, L. (2018) Certificateless Public Key Signature.	The certificateless public key cryptography handle public keys quickly without certificates and to get rid of the key-escrow property as part of identity-based encryption.	A malicious person cannot generate a valid signature using a victim's public key even if they successfully use a key replacement attack.	The public key no longer entirely consists of the identifying information.	CL-PKS has greater security than existing scheme

Tab. 3 Comparative Analysis of four certificateless schemes

In tab.2 Show the comparative analysis of four certificateless schemes in terms of strength, weakness and design model these are Certificateless Signcryption Scheme from Lattice, Certificateless Homomorphic Signature Scheme for Network Coding, Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices, Certificateless Public Key Signature.

System design

Fig 3. Show the flowchart process of the signing a document and generating a digital signature and how the message is verifier.

Message signing **Message verification signature**

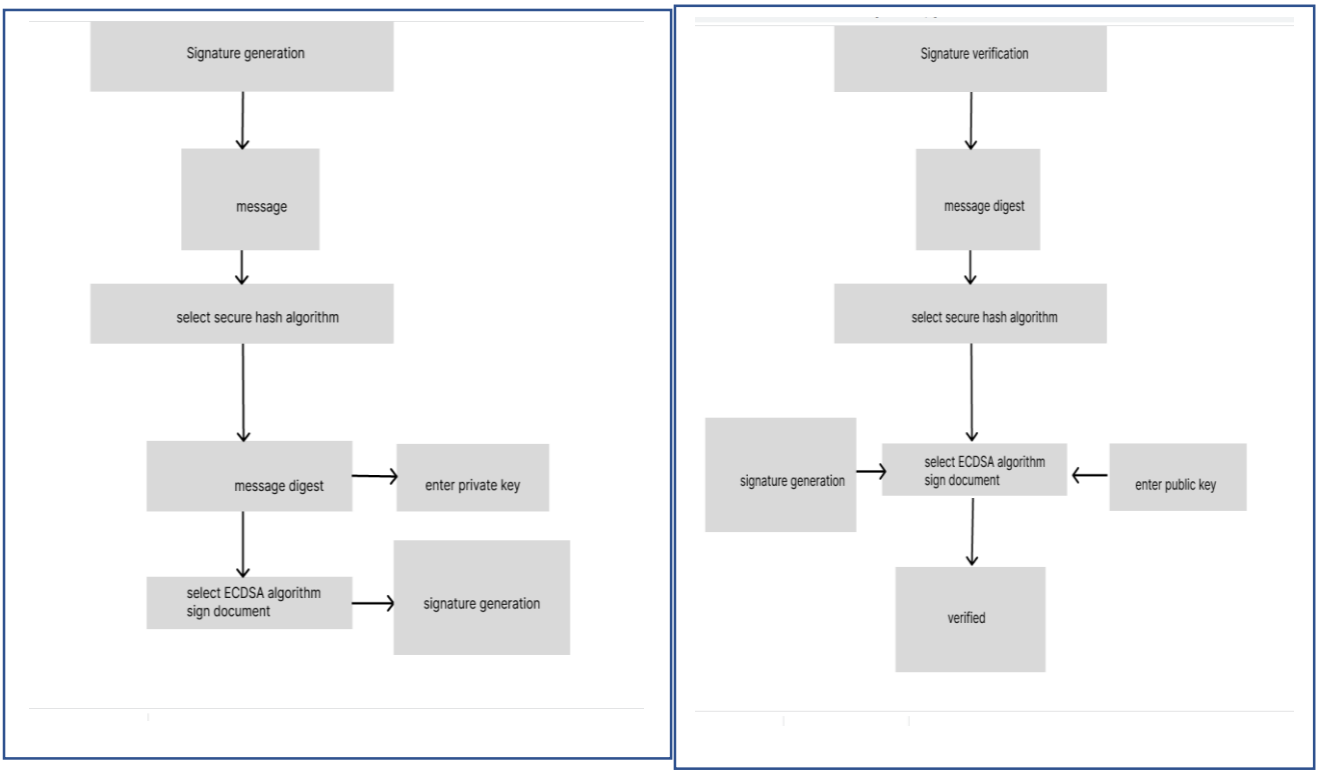

Figure 3 Message signing -digital signature and verification message signing

SOFTWARE PLATFORM

Docker container: Software is delivered in packages known as containers utilizing OS-level virtualization via a collection of platforms as a service technology known as Docker.

Python: The programming language Python is high-level and versatile. Code readability is a priority in its design philosophy, which uses substantial indentation. Both Python's types and trash collection are dynamic. It is compatible with a variety of programming paradigms, including structured, object-oriented, and functional programming.

API: The word "API" refers to a software interface that enables two apps to communicate with one another.

OpenSSL: A software library called OpenSSL is used by programs to protect communications across computer networks from listening devices or the requirement to identify the other side.

The main strength of the OpenSSL library is its support for the usage of public key cryptography for automatically encrypting or verifying data.

Implementation of the best-proposed certificateless identification technique, **elliptic curve digital signature-based certificateless public key signature scheme.**

Since it is based on elliptic curve cryptography and provides a higher level of security with a smaller key size than other signature methods, elliptic curve digital signature is more effective than other signature approaches.

Elliptic Curve Cryptography

The keys for the Elliptic Curve Digital Signature Algorithm, Digital Signature Algorithm, are produced using elliptic curve cryptography. It is a particularly powerful equation based on public key cryptography.

Elliptic Curve Digital Signature Algorithm, which is commonly used in encrypted messaging apps and other security systems, is the cornerstone of Bitcoin security.

In Transport Layer Security, the Secure Sockets Layer's replacement, connections between web browsers and online programs are also encrypted using elliptic curve digital signatures. The image of a real padlock displayed in the browser illustrates how signed certificates using the elliptic curve digital signature algorithm establish an encrypted connection to a hypertext transfer protocol safe website.

The Elliptic Curve Digital Signature Algorithm is a public key encryption scheme that is among the most challenging ones. Compared to digital signing methods, elliptic curve cryptography typically generates keys that are smaller. Elliptic curve cryptography is a form of public key cryptography that relies on the algebraic structure of finite fields. Digital signatures and pseudo-random numbers, among other things, are mostly produced using elliptic curve cryptography. In a digital signature, an authentication method, the sender's identity is verified by using a public key pair and a digital certificate as a signature.

A secure digital signature system in terms of cryptography is the elliptic curve digital signature algorithm. The mathematical underpinnings of the elliptic-curve discrete logarithm problem are the cyclic groups of elliptic curves over finite fields and the complexity of the elliptic-curve discrete logarithm problem issue. The elliptic curve point multiplication-based elliptic curve digital signature algorithm sign/verify algorithm is described in the following. Elliptic curve digital signature methods produce keys and signatures that are shorter than RSA for the same level of security. A 3072-bit RSA signature has the same level of security as a 256-bit ECDSA signature.

Key Generation

The public key is publKey = privKey * G and the private key is privKey.

The private key is generated using random integers in the [0...n-1] range. The public key publKey, which is a point on the elliptic curve, is produced by multiplying an EC point: publKey = privKey * G. (the private key, multiplied by the generator point G).

The public key EC point "x, y" can be compressed using one of the coordinates plus one bit (parity). The secp256k1 curve's compressed public key is a 257-bit integer, or roughly 33 bytes, while the private key is a 256-bit integer, or roughly 32 bytes.

Signature

Calculating the message hash using a cryptographic hash function, such as SHA-256: h = hash (msg) Make k with a safe random number generator in the range [1..n-1].

For deterministic-ECDSA, the value k is obtained from h + privKey using HMAC.

Find the random point's x-coordinate using the formula R = k * G: r = R.x

Execute the following signature proof: s=k-1*(h+r*privkey) (mod n),

As the modular inverse k-1(mod n) is an integer, return the signature "r, s" because k*k-1 1. (mod n) The range of values for each integer in the calculated signature pair [r, s] is [1...n-1]. It encrypts the random point R = k * G and includes a proof s that the signer is aware of the message h and the private key privKey. The proof utilizing concept can be validated using the supplementary publKey. Elliptic curve digital signatures have a curve twice as long as the private key of the signer. For 256-bit elliptic curves (like secp256k1), the ECDSA signature is 512 bits (64 bytes), and for 521-bit curves, it is 1042 bits (like secp521r1).

Verifying signature

The public key pub, the signed message msg, the signature r, s produced by the signing algorithm, and All of the inputs to the procedure required to validate an elliptic curve digital signature are keys, which correspond to the signer's private key. Authentic or false signature is the resultant Boolean value. This is how the algorithm used to validate digital signatures using elliptic curves works. Calculate the message hash using the same cryptographic hashing technique as used for signing: h = hash (msg) Calculate the modular inverse of the signature proof: s1 = Retrieve the random point associated with signing: r * s1 * publKey = R' h * s1 * G from R', determine its x-coordinate: r' = R'.x to determine the outcome of the signature validation, compare if r' == r.

Hash Function

Elliptic curve digital signature before being encrypted, the message must first be hashed.

Hashing

A hash function is a mathematical procedure that converts one input numerical value into another. Although the hash function's input might be any length, its result is always a defined length. The terms used to describe the values that a hash function produces are message digests.

Features

The hash function can be used to reduce data of arbitrary length to a fixed length. This method is referred to as data hashing. Since hash values are sometimes much less than the input data, hash functions are sometimes referred to as compression functions. Given that it is a compressed representation of a larger piece of data, a hash is also referred to as a digest. A hash function with an output of n bits is referred to as an n-bit hash function. Common hash functions produce results in the 160-to-512-bit range.

Properties

This property suggests that reversing a hash function ought to be computationally difficult. If a hash function h generated a hash value z, it is very difficult to find any input value x that hashes to z. This feature protects against an attacker who is only armed with the input's hash value and trying to locate it. According to the property, given an input and its hash, it should be challenging to find an alternative input with the same hash. In other words, if a hash function h produces a hash value h(x) given an input x, it should be difficult to find any additional input value y such that h(y) Equals h. (x).

Collision

Given this, comparing two inputs with different durations that create the same hash should be difficult. This trait is also known as "collision-free hash function". It is difficult to find any two distinct inputs x and y such that h(x) = h for a hash function h, in other words (y). To make sure that message M's content hasn't changed, utilize the hash function. Output value h will change if the material is altered in any way. Therefore, it's employed in numerous industries, including digital forensics and digital signature, to guarantee information security. The hash algorithm must have qualities that make one-way traffic safe and collisions unlikely. The attribute known as collision ensures that the same output hash value, h, is generated for various input message values.

It is difficult for a hash function to be collision-free because it compresses data with a set hash length. These collisions should be difficult to locate, as this attribute of collision-free simply serves to affirm. This feature makes it extremely difficult for an attacker to separate two input values with the same hash. A hash function is also resistant to second pre-images if it is collision resistant. M_1 M_2, H (M_1) = H (M_2) When creating a signature, the input message is a hash, which produces a value known as the hash digest. Next, a secret authentication key is entered, and last, the signature function ECDSA is chosen to create the signature. Key length of hash is 512 bits.

Fig.4 The user uploads a document, the hash function is chosen to convert the document into a message digest, the signature function (ECDSA) is chosen, and the signature is created. In step 5, the verifier validates the signature by reverse-encrypting the hash value.

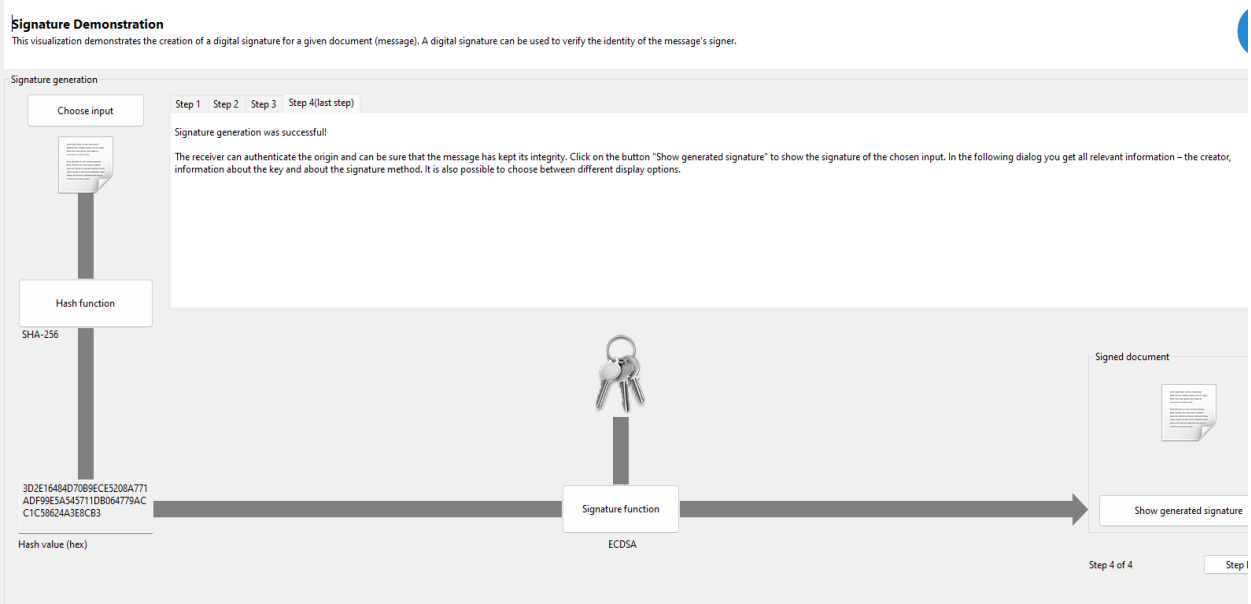

Figure 4 : Digital signature demonstration

Fig.5 Display the produced signature, the owner of the signature, the key and signature techniques used, the length of the signature (54 bytes), the length of the message being signed, and the message itself.

Digital signature

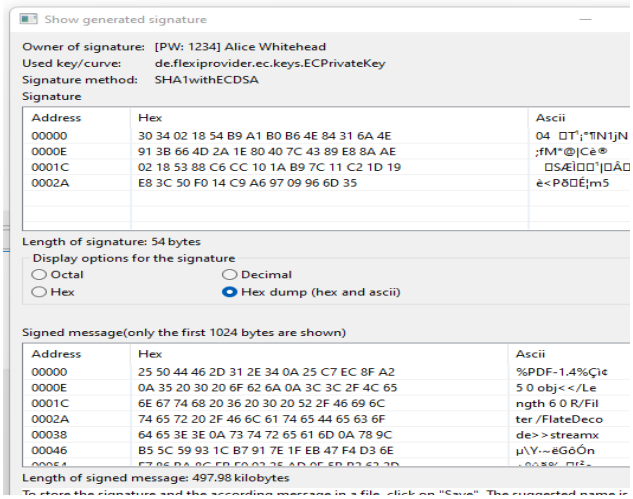

Figure 5 Generated digital signature

Fig.6 Display the verification process; a verified signature is entered; SHA-256 is chosen as the hashing algorithm. Choose the ECDSA hash match verification option to confirm the authenticity of the signature.

Figure 6 Demonstration of signature verification

The verification result of generated signature.

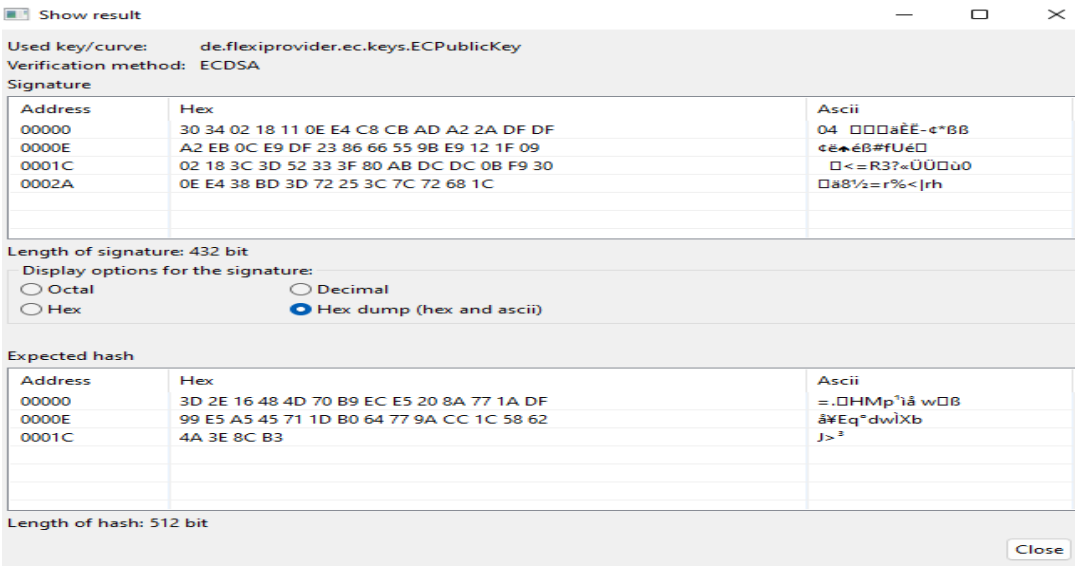

Figure 7 output of verification signature

Digital Data States

Table 4:

Data State	Data Explantations
Data in transit	Data transmission such as Email, email attachments document, Memos, and many more, sync files.
Data at rest	Data retention such as corporate contract documents, account statement memos, archive files

Tab.3 Digital data state

In tab.3 Show the phases of digital data state at which encryption is employed to safeguard data privacy both during storage and transmission.

RESULT AND DISCUSSION

The deployment is tested on a computer with an Intel(R) Core (TM) i7-8700 CPU running at 3.20GHz and 3.19GHz, hosting virtual machines with Ubuntu 15.04 operating system, and providing execution time metrics. Using the dynamic analysis tool Veracode, the software is put in a docker container running on Ubuntu and tested for memory-related issues. The implementation of elliptic curve cryptography with help from the elliptic curve digital signature algorithm. The programming language used in the implementation environment is Python, which is available under the MIT license. The library creates the signing and verifying keys for the messages, signs them, and validates their signatures. It provides five well-known NIST prime field curves with key lengths of 192, 224, 256, 521 bits as well for key synthesis, signing, validating, and shared secret derivation. These curves are listed as prime 192v1, secp224r1, prime 256v1, secp384r1, and secp521r1 by the OpenSSL tool (OpenSSL param -list curves). This library's functions for key generation, signing, verifying, and shared secret derivation work with the NIST "Suite B" GF(p) (prime field) curves with keys that are 192, 224, 256, 384, and 521 bits long. These curves have been given the "short names" Prime 192v1, Secp 224r1, Prime 256v1, Secp 384r1, and Prime 521r1 by the OpenSSL tool (openssl param -list curves). For Brain pool curves, the bit range of 160 to 512 is also supported. These are the typical (untwisted) varieties. BrainpoolP160r1, BrainpoolP192r1, BrainpoolP224r1, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1, and BrainpoolP512r1 are the "short names" for these curves. Among the ever-growing number of network-connected gadgets are ones for the internet of things. These devices don't have usernames or passwords to identify themselves or their function on the network, so access to them can be controlled using certificateless public key infrastructure. This gives them just the right amount of network access to perform their function while maintaining data privacy and security. They are simple to manage since the keys and signatures are so short.

RESULT OUTPUT:

Message signature:

Elliptic curve key generates: secp256k1

Private key output generated

-----BEGIN EC PRIVATE KEY-----

MHQCAQEEIAB0VlFG3UGXhDU9yNqks01OrR7nGONn
xan3zfUQlTOWoAcGBSuBBAAK
oUQDQgAESs9myr9JJEyLIUkoWmIhalz6CPOi/CxBf4sk+
G17Uig8YY9Za2SKtzgo

06Hplhvfu8MVizrzYyvx1yaH+TLoPg==
-----END EC PRIVATE KEY-----

Public key output generated

-----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAESs9myr9J
JEyLIUkoWmIhalz6CPOi/CxB
f4sk+G17Uig8YY9Za2SKtzgo06Hplhvfu8MVizrzYyvx1ya
H+TLoPg==
-----END PUBLIC KEY-----

Plain text messages: "Among the ever-growing number of network-connected gadgets are ones for the internet of things. These devices don't have usernames or passwords to identify themselves or their function on the network, so access to them can be controlled using certificateless public key infrastructure. This gives them just the right amount of network access to perform their function while maintaining data privacy and security."

Output digital generated signature of the message signed.

MEYCIQCJS+prs9sH2Yfgs/ytQgiT2JE9ML/IWgx/Rr7c6qv
d6gIhAOtzzJEEDUiTGEELMoQsRGfn4kFgjTwdLXu9cEu
JGHmM

Signature verification output for verifying the digital signature

MEYCIQCkBsV0qWRvhd5aeCNxVwYEHMeEDY7f5ReK
QP5lZNDZPwIhAMaP9pGBxdlTE5w4KTOok2aTsOW3v4
9z7fvqC/4iyvoe

CONCLUSION

To protect and authenticate the data privacy of people and government organizations, this paper provided a workable implementation of a certificateless encryption technique combining elliptic curve cryptography and elliptic curve digital signature creation. While maintaining the same degree of security, elliptic curve digital signatures provided smaller keys than traditional techniques like RSA (Rivest-Shamir Adleman). The pragmatic findings showed how elliptic curve digital signatures can be used to protect data both during transmission and at storage. Combining entities for encryption, digital signature ensures complete data privacy in the government information technology domain.

REFERENCE

1. Ahmad, N. M. et al. (2011) 'Comparative analysis and implementation of certificateless based authentication scheme', Communications in Computer and Information Science, 251 CCIS(PART 1), pp. 151–162. doi: 10.1007/978-3-642-25327-0_14.
2. B, Z. C. and Chen, L. (2018) Certificateless Public Key Signature. Springer International Publishing. doi: 10.1007/978-3-319-99807-7.
3. Chang, J. et al. (2020) 'Certificateless Homomorphic Signature Scheme for Network Coding', IEEE/ACM Transactions on Networking, 28(6), pp. 2615–2628. doi: 10.1109/TNET.2020.3013902.
4. Cui, B. bei, Wei, L. and He, W. (2022) 'A New Certificateless Signcryption Scheme for Securing Internet of Vehicles', SSRN Electronic Journal, pp. 0–19. doi: 10.2139/ssrn.4019225.
5. Fidelis, C. and Borjas, H. (2020) 'Certificateless Identification of Wireless Sensor Nodes', (December 2019).
6. Gautam, S., Gaur, S. S. and Masood, S. (2019) 'A comparative study of certificate and certificate-less cryptographic algorithm and its energy consumption analysis in WSN', TARU Journal of Computer Dynamics & Technological Advances, 1(2, 3, 4), pp. 85–100. doi: 10.47974/2019.tjcdta.004.
7. Genc, Y. and Afacan, E. (2021) 'Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA)', 2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021 - Proceedings. doi: 10.1109/IEMTRONICS52119.2021.9422589.
8. Ghani, R. F. et al. (2022) 'Blockchain-based student certificate management and system sharing using hyperledger fabric platform', Periodicals of Engineering and Natural Sciences, 10(2), pp. 207–218. doi: 10.21533/pen.v10i2.2839.
9. Ibraheem, I. N., Hassan, S. M. and Abead, S. A. (2020) 'Comparative analysis & implementation of image encryption & decryption for mobile cloud security', International Journal of Advanced Science and Technology, 29(3 Special Issue), pp. 109–121.
10. Li, J. (2022) 'Comparative Analysis of Some Typical Encryption Algorithms and Hash Algorithms', Proceedings - 2022 International Conference on Big Data, Information and Computer Network, BDICN 2022, pp. 27–30. doi: 10.1109/BDICN55575.2022.00013.
11. Makarenko, I. et al. (2020) 'A Comparative Analysis of Cryptographic Algorithms in the Internet of Things', 3rd International Science and Technology Conference 'Modern Network Technologies 2020', MoNeTeC 2020 - Proceedings. doi: 10.1109/MoNeTeC49726.2020.9258156.
12. Mandal, S. et al. (2020) 'Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment', IEEE Internet of Things Journal, 7(4), pp. 3184–3197. doi: 10.1109/JIOT.2020.2966242.
13. Mwitende, G. et al. (2020) 'Certificateless authenticated key agreement for blockchain-based WBANs', Journal of Systems Architecture, 110, p.

101777. doi: 10.1016/j.sysarc.2020.101777.

14. Peng, C. et al. (2021) 'Efficient Certificateless Online/Offline Signature Scheme for Wireless Body Area Networks', IEEE Internet of Things Journal, 8(18), pp. 14287–14298. doi: 10.1109/JIOT.2021.3068364.
15. People, D. (no date) 'Constructing a pairing-free certificateless proxy signature scheme from ECDSA', pp. 1–33.
16. Semal, B., Markantonakis, K. and Akram, R. N. (2018) 'A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks', AIAA/IEEE Digital Avionics Systems Conference - Proceedings, 2018-September, pp. 1–8. doi: 10.1109/DASC.2018.8569730.
17. Tajammul, M., Parveen, R. and Tayubi, I. A. (2021) 'Comparative analysis of security algorithms used in cloud computing', Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021, pp. 875–880. doi: 10.1109/INDIACom51348.2021.00157.
18. Take, S. N. and Rokade, P. M. D. (2021) 'Customized E-Certification Generation using Blockchain Technology for Distributed Framework', (4), pp. 442–446.
19. Tan, H., Gui, Z. and Chung, I. (2018) 'A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs', IEEE Access, 6(c), pp. 74260–74276. doi: 10.1109/ACCESS.2018.2883426.
20. Tedeschi, P. et al. (2020) 'LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications', IEEE Internet of Things Journal, 7(1), pp. 621–638. doi: 10.1109/JIOT.2019.2953549.
21. Thumbur, G. et al. (2021) 'Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks', IEEE Internet of Things Journal, 8(3), pp. 1908–1920. doi: 10.1109/JIOT.2020.3019304.
22. Toradmalle, D., Muthukuru, J. and Sathyanarayana, B. (2019) 'Certificateless and provably-secure digital signature scheme based on elliptic curve', International Journal of Electrical and Computer Engineering, 9(4), pp. 3228–3231. doi: 10.11591/ijece.v9i4.ppxx-xx.
23. Xu, Z. et al. (2020) 'Efficient Certificateless Aggregate Signature Scheme for Performing Secure Routing in VANETs', Security and Communication Networks, 2020. doi: 10.1155/2020/5276813.
24. Yu, H. et al. (2021) 'Certificateless Signcryption Scheme from Lattice', IEEE Systems Journal, 15(2), pp. 2687–2695. doi: 10.1109/JSYST.2020.3007519.
25. Yu, H. and Li, W. (2020) 'A certificateless signature for multi-source network coding', Journal of Information Security and Applications, 55(October), p. 102655. doi: 10.1016/j.jisa.2020.102655.
26. Zhang, P. et al. (2022) 'An ECC-Based Digital Signature Scheme for Privacy Protection in Wireless Communication Network', Wireless Communications and Mobile Computing, 2022. doi: 10.1155/2022/1977798.
27. (People, no date; Ahmad et al., 2011; B and Chen, 2018; Semal, Markantonakis and Akram, 2018; Tan, Gui and Chung, 2018; Toradmalle, Muthukuru and Sathyanarayana, 2019; Gautam, Gaur and Masood, 2019, 2019; Makarenko et al., 2020; Mandal et al., 2020; Mwitende et al., 2020; Chang et al., 2020; Tedeschi et al., 2020; Xu et al., 2020; Yu and Li, 2020; Fidelis and Borjas, 2020; Ibraheem, Hassan and Abead, 2020; Peng et al., 2021; Tajammul, Parveen and Tayubi, 2021; Take and Rokade, 2021; Thumbur et al., 2021; Yu et al., 2021, 2021; Genc and Afacan, 2021; Li, 2022; Zhang et al., 2022; Cui, Wei and He, 2022; Ghani et al., 2022).