DATA PRIVACY, SECURITY & CRYPTOLOGY

Anamika Saini[1]*, Dr. Kavita Rathi[2]

Abstract
Data security is a critical aspect of modern information technology and business practices. It is essential for protecting sensitive information, ensuring business continuity, complying with regulations, and maintaining customer trust. By employing encryption, access controls, firewalls, and other security measures, organizations can strengthen their data security posture and defend against evolving cyber threats.

The article reviews the Data security and application of Cryptology for security

Keywords: Data Privacy,Security, Cryptology, Secure Communication

[1]*Research Scholar, Deen Bandhu Chotu Ram University of Science & Technology Sonipat, India
Email: Sainianamika.anu@gmail.com
[2]Assistant Professor, Deen Bandhu Chotu Ram University of Science & Technology Sonipat, India
Email: Kavitarathi.cse@dcrustm.org

***Corresponding Author: Anamika Saini**
*Research Scholar, Deen Bandhu Chotu Ram University of Science & Technology Sonipat, India
Email: Sainianamika.anu@gmail.com

DOI: 10.53555/ecb/2022.11.12.304

I. INTRODUCTION

In the current era interconnected and a world that relies on data, the concept of data privacy has become a critical concern for everyone [1]. With the proliferation of the digital era and the widely spread collection, storage, and analysis of personal data, protecting individuals' privacy has emerged as a paramount challenge [2].This chapter provides a comprehensive overview of data privacy, discussing its importance, the challenges it faces, and the solutions devised to safeguard sensitive information [3.] By delving into the legal, technical, and ethical aspects of data privacy, by reading these chapters different readers with the knowledge necessary to navigate the evolving landscape of data privacy in the digital era [4]. As well as security is also an important aspect when we talk about digital data transmission.

Safeguarding digital data, disclosure, alteration/changes, or destruction/deletion [5]. It entails putting in place measures for safeguard sensitive information and ensue the availability, integrity and confidentiality of data. Data security is essential in various sectors to protect valuable information, maintain trust, comply with regulations, and prevent data breaches and cyber-attacks [6].

Cryptology is also a term that is used for secure communication over the internet as well as in earlier times different techniques are used for secure communication [7]. So in conclusion we can say privacy and security are very important and cryptology helps us to achieve these terms. Let's discuss all of these in detail.

II. DATA PRIVACY

A. Defination

It's an area of data protection also called information privacy or data privacy that is used for the proper handling of different types of the data like personal, financial, property, confidential data, etc. The different fields like information security, computer security, and data security all are designed to solve this data privacy issue. Data privacy is crucial to maintaining trust between data collectors and data subjects, fostering a secure environment for the exchange of information [8].

B. Need of Data Privacy

- **Individual Autonomy**: Data privacy allows individuals to have control over their personal information, enabling them to make informed decisions about how their data is being used by anyone.
- **Trust and Reputation**: Organizations that prioritize data privacy gain trust from customers and stakeholders, which enhances their reputation and credibility [9].
- **Preventing Misuse**: Data privacy measures help prevent the misuse of personal information for malicious purposes, such as fraud, identity theft, etc.
- **Legal Compliance**: With the increasing number of data protection laws and regulations worldwide, organizations must comply with these laws to avoid legal repercussions and penalties [10].
- **Business Competitiveness**: Demonstrating a commitment to data privacy can become a competitive advantage as customers tend to choose organizations that respect their privacy.

C. Legal Framework of Data Privacy

The legal framework governing data privacy encompasses legislation, regulations, and guidelines that oversee the acquisition, retention, utilization, and dissemination of individual data by various entities, including organization and government bodies [11]. The legal framework for data privacy varies from country to country, and in some cases, regions or states within a country may have their own specific regulations [12]. Here are some key components commonly found in data privacy legal frameworks:

- **Data Protection Laws**: Data protection laws typically define what constitutes personal data, the rights of data subjects (individuals whose data is being collected), and the responsibilities of data controllers and data processors (organizations handling the data) [13].
- **Data Security and Confidentiality**: Data protection laws often mandate that organizations implement appropriate security measures to safeguard personal data from unauthorized access, disclosure, or loss [14]. Organizations are also required to maintain the confidentiality of personal data and take steps to prevent data breaches.
- **Data Transfer and Sharing**: Some data privacy laws include provisions regarding the transfer of personal data across international borders or to third-party organizations [11]. Adequate safeguards must be in place to ensure that data transferred to other countries or entities maintains the same level of protection as required by the originating country's laws.
- **Regulatory Authorities**: Data privacy laws typically establish regulatory bodies or data protection authorities responsible for enforcing the law, conducting investigations, and imposing penalties for non-compliance [15].

- **Consent and Purpose Limitation**: Data protection laws often require organizations to obtain explicit and informed consent from person before assembling and processing their personal data [16]. The reason for which the data is gathered must be clearly stated, and the data cannot be used for any other purposes without obtaining additional consent.
- **Data Subject Rights**: Data protection laws typically grant certain rights to individuals regarding their personal data [17]. These rights may include the right to use, to correct, to correct & to restrict their data.
- **Data Breach Notification**: Some data protection laws need organizations to report data violation to related officials and affected person within a specified timeframe [10]. This ensures that individuals are informed of potential risks and can take appropriate actions to protect themselves.

It is requisite for organizations to be aware of and comply with the data privacy legal framework applicable to their operations to ensure they handle personal data in a lawful and ethical manner [18]. Failure to comply with data privacy laws can lead to severe financial penalties and reputational damage.

D. Data Privacy Challenges

Data privacy faces numerous challenges in the digital age due to the ever-evolving landscape of technology, data collection, and global interconnectedness [19].Some of the key challenges in data privacy include:

- **Data Breaches**: One of the most significant challenges is the increasing number of data breaches. Cyber-attacks and data breaches can lead to unauthorized access to personal information, resulting in identity theft, financial fraud, and reputational damage for individuals and organizations [20].
- **Big Data and Analytics**: The cluster and survey of vast amounts of data raise privacy concerns. [21]Big data analytics can reveal sensitive information and patterns that individuals may not want to be disclosed, even if the data is anonym zed.
- **Internet of Things (IoT**): The proliferation of these devices which has iot introduces new privacy risks as these devices collect and share data about individuals' behaviors, habits, and preferences [22].
- **Social Media and Online Platforms**: Social media platforms and online services collect extensive user data, which can be used for targeted advertising and profiling. Users may not always be aware of the extent of data collection or the ways their information is used [23].
- **Cross-Border Data Transfers**: Data is often transferred across international borders, and different countries may have varying data protection laws and standards, making it challenging to ensure consistent and adequate data privacy measures.
- **Lack of Awareness and Informed Consent**: Many individuals are not fully aware of how their data is gathered, used, and shared, and may unknowingly provide consent without understanding the implications.
- **Privacy Policies and Terms of Service**: Lengthy and complex privacy policies & terms of service can discourage users from reading them thoroughly, leading to potential misunderstandings about data handling practices [24].
- **Third-Party Data Sharing**: Data is often shared with third-party vendors or partners, raising concerns about how well these entities protect the data and whether they adhere to privacy regulations [25].
- **Government Surveillance**: Mass surveillance programs and access to personal data by governments can undermine privacy rights and raise concerns about civil liberties and individual freedoms [26].
- **Privacy in Healthcare and Medical Data**: Protecting sensitive medical data is crucial, but the increasing use of electronic health records and health-related apps poses privacy risks [27].
- **Cultural and Ethical Differences**: Different cultures and ethical perspectives on privacy can influence how individuals and organizations handle personal data, making global data privacy compliance challenging [28].
- **Balancing Privacy and Innovation**: Striking a balance between protecting privacy and enabling innovation and data-driven services is a continuous challenge for policymakers and businesses.[25]

Tracking these challenges necessitates a multi-faceted strategy that involves comprehensive data protection laws, robust security measures, transparency in data handling practices, user education, and ethical considerations in data collection and usage. Organizations and governments must work together to develop effective strategies that safeguard individuals' privacy rights while promoting responsible data practices in the digital era.

E. Data Privacy in the Era of Machine Learning and AI

Future trends and emerging technologies for data privacy are continually evolving to address the complex challenges posed by advancing digital landscapes and increasing data collection. Here are some key developments to look out for:

- **Privacy preserving data analysis**: Differential privacy is a mathematical framework that aims to add noise to datasets to protect individual privacy while still providing accurate aggregate results [29]. It is gaining traction in privacy-conscious industries like healthcare and finance.
- **Privacy-Enhancing Tools and Apps**: We can expect an increase in privacy-focused tools and apps that empower individuals to control their data and monitor its usage across various platforms [30].
- **Block chain and Distributed Ledger Technologies (DLT**): Block chain and DLT can offer enhanced data privacy by enabling decentralized, tamper-resistant, and transparent record-keeping, making data breaches more difficult [31].
- **Privacy Laws and Global Harmonization**: Privacy regulations are continuously evolving worldwide [32]. We may see further updates and a push for global harmonization of data protection laws to facilitate international data transfers.
- **Biometric Privacy**: As biometric technologies become more widespread, there will be a greater emphasis on safeguarding biometric data, such as fingerprints and facial scans, from unauthorized access [33].
- **Privacy in Artificial Intelligence (AI)**: Ensuring privacy in AI applications, especially in fields like natural language processing and computer vision, will be a priority to mitigate risks of data exposure and misuse [34].
- **Decentralized Identifiers (DIDs) and Self-Sovereign Identity (SSI**): DIDs and SSI aim to provide individuals with full control over their identity data, reducing reliance on centralized identity management systems [35].
- **Contextual Privacy**: Contextual privacy focuses on tailoring data privacy measures to the specific context in which data is collected, used, and shared, considering factors like the data subject's preferences and the sensitivity of the information [36].
- **Privacy Auditing and Certifications**: Privacy auditing and certification services may emerge to help organizations demonstrate compliance with privacy standards and reassure customers about their data protection practices [37].
- **Quantum-Safe Cryptography**: With the potential threat of quantum computers breaking conventional cryptographic methods, the adoption of quantum-safe cryptography will become essential to secure sensitive data in the future [38].
- **Ethical Data Use and AI Governance**: Organizations will focus on establishing comprehensive AI governance frameworks that ensure responsible data use and ethical AI development [39].
- **Privacy Regulations for Emerging Technologies**: As new technologies emerge, regulators will likely respond with specific privacy regulations to address the unique challenges they pose.

The future of data privacy will be shaped by a combination of technological advancements, evolving legal landscapes, and societal demands for greater control over personal data. Striking a balance between innovation and privacy protection will be a critical challenge for businesses, policymakers, and technologists as they navigate this dynamic landscape.

F. Managing Privacy with Today's Requirements

- **Privacy by Design**: Integrate privacy considerations into every stage of system development; ensuring data protection is a fundamental part of any product or service [40].
- **Transparent Data Practices**: Clearly communicate data collection, use, and retention policies to users, obtaining explicit consent whenever necessary.
- **Data Minimization**: Collect only the data that is essential for the intended purpose and avoid retaining it longer than required.
- **Security Measures**: Implement robust security protocols, including encryption, access controls, and regular security audits, to protect data from unauthorized access.
- **Data Breach Response Plan**: Develop a comprehensive plan to respond to data breaches promptly and responsibly, minimizing the impact on affected individuals [41].
- **Educating Employees**: Train employees about data privacy best practices and their responsibilities in handling sensitive information.
- **Collaboration with Third Parties**: If data is shared with third-party vendors, ensure they also comply with privacy regulations and adhere to industry best practices.

- **Continuous Improvement**: Stay updated with the latest trends, technologies, and regulations related to data privacy and make necessary adjustments to privacy policies and practices accordingly.

By following these principles and adopting a proactive approach to data privacy, organizations can build a strong foundation for protecting individuals' sensitive information and fostering a culture of trust and responsibility in the digital ecosystem.

G. Advantages of Data Privacy:

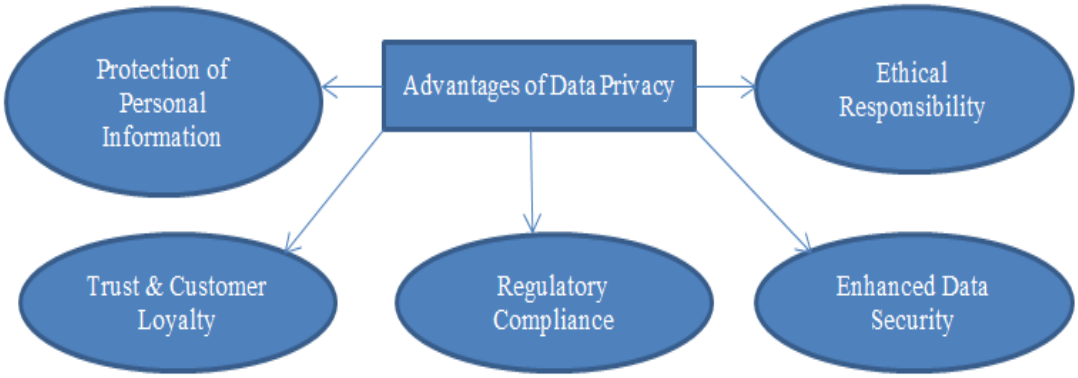

Figure 1: Advantages of Data Privacy

- **Protection of Personal Information**: Data privacy safeguards sensitive data by protecting personal information [42].
- **Trust and Customer Loyalty**: Privacy-conscious organizations build trust with customers, leading to stronger brand loyalty.
- **Regulatory Compliance**: Following data privacy regulations ensures that organizations avoid legal troubles and penalties [43].
- **Enhanced Data Security**: Privacy measures often involve strengthening data security practices, reducing the likelihood of data breaches.
- **Ethical Responsibility**: Respecting data privacy demonstrates ethical behavior and social responsibility.

H. Disadvantages of Data Privacy

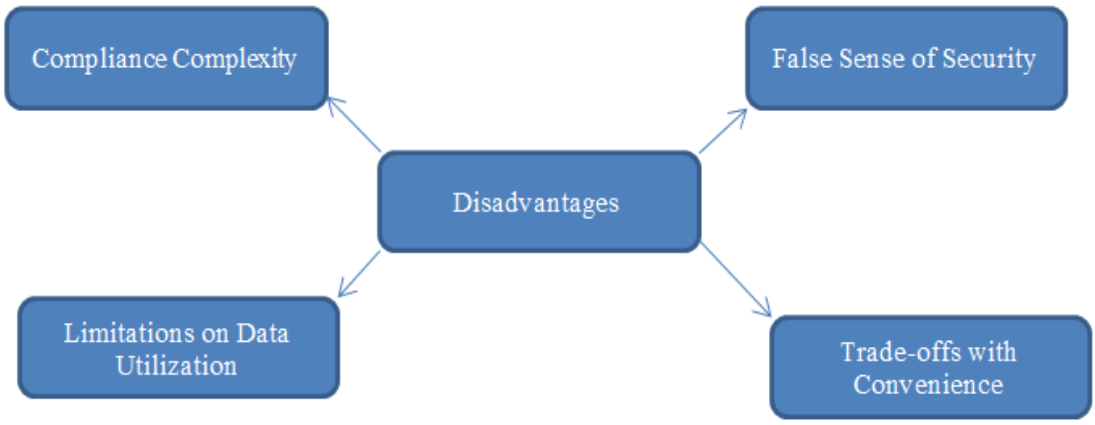

Figure 2: Disadvantages of Data Privacy

- **Compliance Complexity**: Meeting data privacy regulations can be challenging and resource-intensive for organizations, especially those operating globally.
- **Limitations on Data Utilization**: Strict privacy regulations may limit the ways organizations can use data for analysis and research, potentially hindering innovation.
- **Trade-offs with Convenience**: Enhanced data privacy measures can sometimes lead to inconvenience for users, such as additional authentication steps.
- **False Sense of Security**: Despite efforts to ensure data privacy, there is no foolproof method to guarantee absolute protection against all potential threats [44].

III. DATA SECURITY

A. Defination

Securing data involves safeguarding it, protecting digital information from accessing by illegitimate person, disclosure, or destruction [6]. It implements measures to safeguard sensitive information and ensure the basic needs of security that is confidentiality, integrity, and availability of data [27]. Data security is essential in various sectors to protect valuable information, maintain trust, comply with regulations, and prevent data breaches and cyber-attacks.

B. Need of Data Security

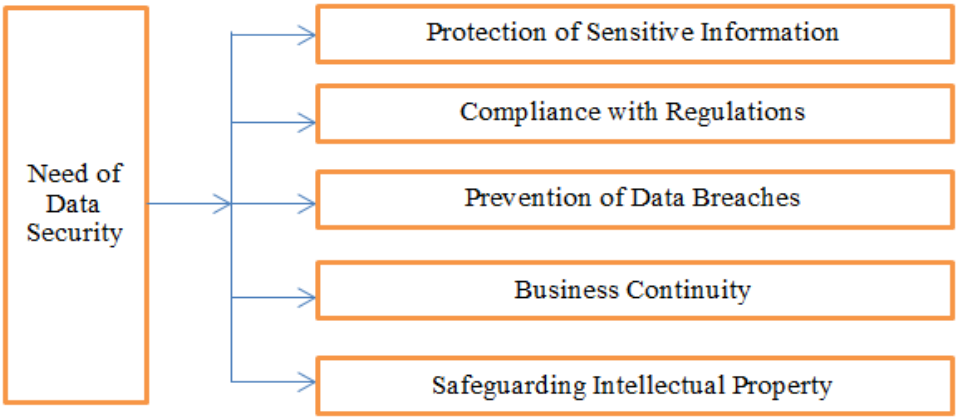

Figure 3: Need of Data Security

- **Protection of Sensitive Information**: Data security is crucial to safeguard sensitive data, such as personal information, financial records, intellectual property, and trade secrets. Failure to protect this data can lead to reputational damage, identity used by fake person, financial fraud etc.[45].
- **Prevention of Data Breaches**: Data breaches can result in significant financial damage, reputational damage. Data securities measures help prevent unauthorized access and data breaches [47].
- **Business Continuity**: Data security is necessary for ensuring the availability & integrity of data, which is essential for the smooth functioning of organizations and maintaining business continuity.
- **Safeguarding Intellectual Property**: Companies need to protect their intellectual property, including research and development data, designs, and proprietary algorithms, from competitors and cybercriminals [48].

C. Requirements of Data Security

Data security is basic aspect of modern information technique and business practices. It is essential for protecting sensitive information, ensuring business continuity, complying with regulations, and maintaining customer trust [49].
By using the things in order which is given in requirements are used for achieving the need of the data security. Let's discuss the different requirements one by one as given in following diagram:

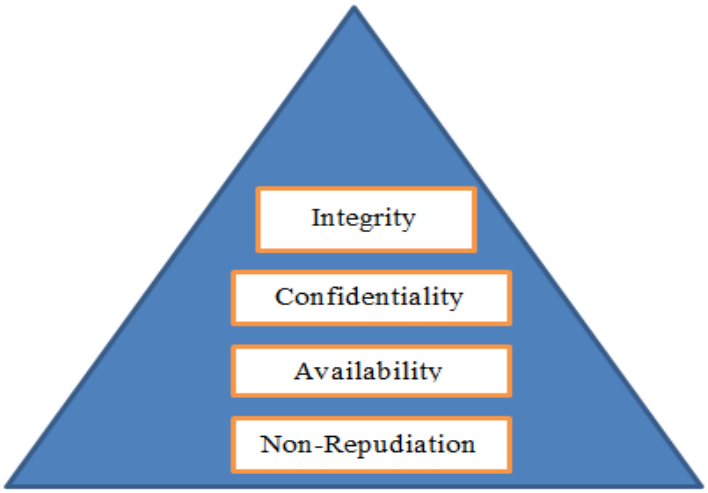

Figure 3: Requirements of Data Security

1. Secrecy: Securing data to restrict access exclusively to authorized individuals or systems. This is achieved through measures like encryption and access controls [50].
2. Integrity: Verifying that data remains unaltered and accurate throughout its lifecycle. Techniques like checksums and digital signatures help ensure data integrity [51].
3. Availability: Ensuring data is accessible to authorized users when needed. Redundancy and backup strategies contribute to data availability.
4. Non-Repudiation: Ensuring that the origin and authenticity of data cannot be denied. Digital signatures and audit trails help achieve non-repudiation [52].

D. Ways to Achieve Data Security

By employing encryption, access controls, firewalls, and other security measures, organizations can strengthen their data security posture and defend against evolving cyber threats. There are different methods available by using them we can achieve the data security. Some of them are following:

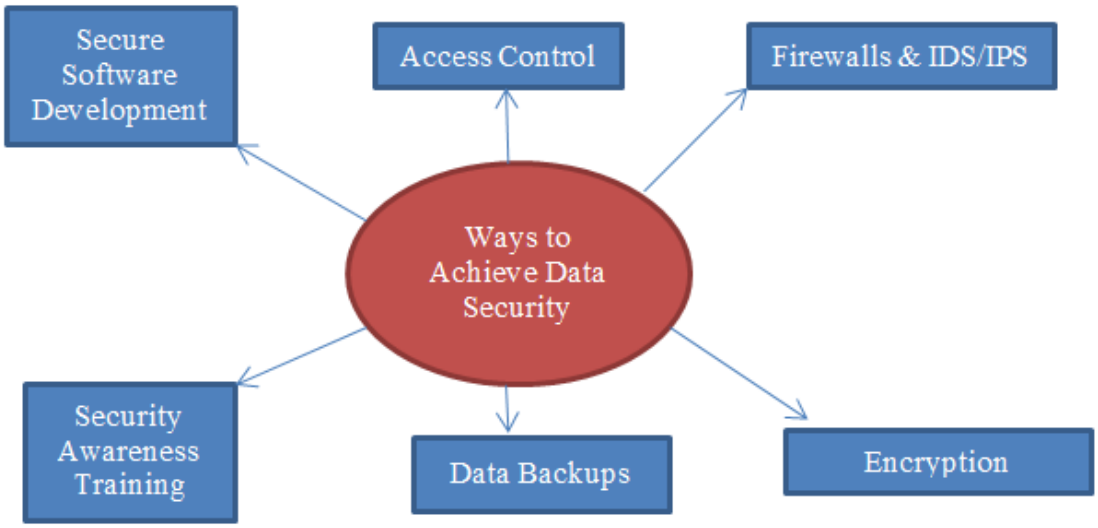

Figure 4: Ways to Achieve Data Security

- **Encryption**: It is a crucial technique used to safeguard sensitive information and protect it from unauthorized access or interception. It involves the process of converting plain, readable data into coded form using different algorithms [40].
- **Access Control**: Implementing access controls ensures that only authorized users have appropriate privileges to access specific data. This includes the use of user authentication mechanisms and role-based access control (RBAC) systems [53].
- **Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):** These security measures protect against unauthorized network access and attacks, such as DDoS (Distributed Denial of Service) attacks and malware intrusions [54].
- **Regular Data Backups**: Regularly backing up data helps recover information in case of data loss due to hardware failures, natural disasters, or ransom ware attacks [55].
- **Training in Security awareness**: Educating employees and users about data security best practices helps prevent social engineering attacks and human errors that can compromise data security.
- **Secure Software Development**: Implementing secure coding practices helps reduce vulnerabilities in software applications, minimizing the risk of data breaches through software exploits [56].

E. Advantages of Data Security

- **Protection Against Data Breaches**: Data security measures protect sensitive information from falling into the wrong hands, preventing potential data breaches and the associated financial and reputational losses [54].
- **Trust and Customer Confidence**: Strong data security practices enhance customer trust and confidence, encouraging them to do business with the organization. This can lead to improved customer loyalty and retention [57]
- **Business Continuity**: Robust data security ensures the availability of critical data, minimizing downtime and ensuring uninterrupted business operations even in the face of potential security incidents [58].

- **Intellectual Property Protection**: Data security safeguards valuable intellectual property from unauthorized access or theft, preserving a company's competitive edge and innovation [59].
- **Competitive Advantage**: Organizations that prioritize data security can gain a competitive advantage by positioning themselves as trustworthy and reliable partners, especially in industries handling sensitive customer data.

IV. CRYPOTOLOGY

A. Defination

Cryptology is the analysis of secure communication techniques, which includes both cryptanalysis & cryptography [60]. It encompasses the science and art of designing, analyzing, and breaking cryptographic systems. The paramount goal of cryptology is to ensure the confidentiality, integrity & authenticity of information while protecting it from unauthorized access and tampering [61].

B. History of Cryptography

The history of cryptography dates back thousands of years, with its roots in ancient civilizations where the need for secure communication and secrecy of information was recognized.[62] Here is a brief overview of the significant milestones in the history of cryptography:

- **Ancient Cryptography**: The earliest known use of cryptography can be traced back to ancient civilizations, including Egypt, Mesopotamia, and Greece. Ancient Egyptians used simple substitution ciphers to encode hieroglyphic messages on monuments, while the Greeks employed the Scytale, a cryptographic device based on a cylinder and a strip of parchment, for military communications [63].
- **Caesar Cipher**: In 58 BCE, Julius Caesar used a simple substitution cipher, now known as the Caesar cipher, to protect his military communications [64].
- **The middle Ages**: During the Middle Ages, cryptography played a significant role in military and diplomatic communications. Various encryption methods, such as the Vigenère cipher, which used a repeating keyword to encrypt messages, were developed and used during this period [62].
- **The Renaissance**: In the 16th century, cryptanalysis (the art of breaking codes) also gained prominence, with the work of notable figures such as Giovanni Battista della Porta and Blaise de Vigenère [63].The efforts to improve encryption techniques led to the development of more complex ciphers.
- **The Enigma Machine**: During World War II, the German military employed the Enigma machine, a sophisticated electromechanical cipher device, to encrypt their communications. Breaking the Enigma code became a critical effort by the Allies and significantly influenced the outcome of the war.
- **The Digital Age**: With the advent of computers in the mid-20th century, cryptography entered a new era. Pioneering works by Claude Shannon and others laid the foundation for modern cryptography. The Data Encryption Standard (DES), introduced in the 1970s, was one of the first widely-used encryption algorithms [65].
- **Public Key Cryptography**: In the mid-1970s, Whitfield Diffie and Martin Hellman introduced the concept of public key cryptography, which two keys – 1st public key for encoding and 2nd private key for decoding [66]. This breakthrough revolutionized secure communication over insecure channels and enabled secure digital signatures.
- **RSA Algorithm**: In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman developed the RSA algorithm, most widely used asymmetric encryption algorithms in modern cryptography [67].
- **Advanced Encryption Standard (AES)**: AES, a symmetric encryption algorithm, became the standard for secure data encryption worldwide. It was adopted by the U.S. government in 2001 and is widely used in various applications [65].
- **Quantum Cryptography**: In recent years, quantum cryptography has emerged as a promising field that leverages the principles of quantum mechanics to create unbreakable encryption methods, such as quantum key distribution [66].

Today, cryptography plays a big role in securing digital communication, securing sensitive information, and ensuring the confidentiality and integrity of data in various applications, ranging from secure websites to financial transactions and digital signatures. The field continues to evolve as new challenges and emerging technologies shape the future of cryptography.

C. Types of Cryptography

Cryptography is a fundamental component of cryptology and involves the use of mathematical algorithms to convert plaintext data into unreadable cipher text, thereby securing the

information during transmission or storage. Encryption is the term for converting plaintext into cipher text, while decryption refers to the reverse process.

Cryptography plays a crucial role in ensuring data privacy and secure communication in various domains. Generally we divide cryptography in two types according the key used for data security as given below:

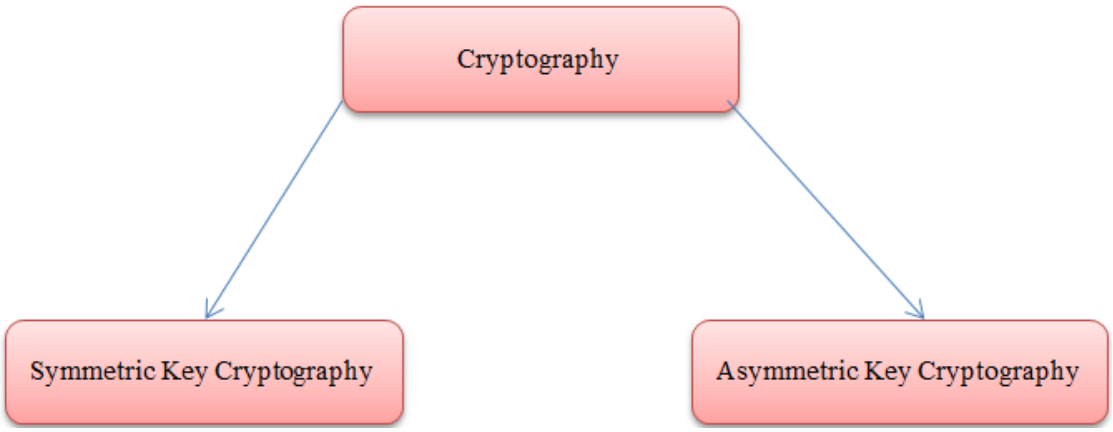

Figure 5: Different types of Cryptography

Cryptography is a fundamental component of cryptology and involves the use of mathematical algorithms to convert plaintext data into unreadable cipher text, thereby securing the information during transmission or storage. The process of converting plaintext to cipher text is known as encryption, and the reverse process is called decryption. Cryptography is instrumental in safeguarding data privacy and establishing secure communication in a multitude of domains.

- **Symmetric Key Cryptography**

It uses a single secret key for both encryption and decryption of data. In this approach, the same key is shared between the sender and receiver, and it must be kept confidential and secure to maintain the confidentiality of the encrypted information [19].

- **How Symmetric Key Cryptography Works?**

Encryption: To encrypt data using symmetric key cryptography, the plaintext (original message) is combined with the secret key using an encryption algorithm, which produces cipher text (encrypted message). The cipher text appears as a seemingly random sequence of characters and cannot be understood without knowledge of the secret key [68].

Decryption: To decrypt the cipher text and retrieve the original plaintext, the receiver uses the same secret key and applies the decryption algorithm, reversing the encryption process. Only with the correct secret key can the cipher text be successfully transformed back into the original plaintext [68].

- **Key Features of using same key:**

Single Key: The primary characteristic is the use of only one secret key for both process encryption and decryption [61].

Fast Computation: Symmetric key algorithms generally have a faster computation speed compared to asymmetric key algorithms, making them more efficient for encrypting and decrypting large volumes of data.

Confidentiality: Symmetric key cryptography ensures the confidentiality of data since the cipher text cannot be understood without knowledge of the secret key [60].

Key Management: The key management in symmetric key cryptography can be challenging, especially when multiple parties need to share the same secret key securely.

Key Distribution: One of the main challenges in symmetric key cryptography is securely distributing the secret key to all parties involved in the communication process, ensuring that unauthorized entities do not gain access to it [32].

- **Several widely used symmetric key encryption algorithms includes the followings:**

DES: A historic symmetric key using algorithm introduced in the 1970s, which uses a 56-bit key length. Due to its small key size, DES is considered relatively weak by today's security standards.

Triple Data Encryption Standard: A advanced version of DES that applies the DES algorithm three times in sequence with different keys, significantly increasing the key length and improving security [69].

Advanced Encryption Standard (AES): The commonly utilized AES algorithm provides robust security and efficient performance through its support key length of 128, 192, and 256 bits [65].

Symmetric key cryptography is commonly used in applications where speed, efficiency, and confidentiality are crucial, such as securing data at rest, securing network communication, and encrypting files and messages [70]. However, its main challenge lies in secure key distribution and management, especially when dealing with a large number of users or parties in a communication network.

- **Asymmetric Key Cryptography (Public Key Cryptography)**

It is a technique that uses a pair of mathematically connected keys for secure communication – a public key and a private key. Asymmetric key cryptography uses two distinct keys for these operations [71].

- **How Asymmetric Key Cryptography Works?**

Public Key: The public key is widely distributed and accessible to anyone. It is used for encrypting plaintext data into cipher text. [72].
Private Key: The private key is kept secret and known only to the owner. It is used for decrypting cipher text back into plaintext. Only the recipient can decrypt the message encrypted with their public key [73].

- **Key Features of using Different Keys:**

Key Pairs: It involves two keys – a public key and a private key. These keys are mathematically connected, but it is computationally not possible to derive one key from the other [40].

Encryption: When someone sends a secret message, they use the receiver's public key to encrypt the message. Once encrypted, the receiver with the corresponding private key can decrypt the message [74].

Digital Signatures: Asymmetric key cryptography enables the creation of digital signatures. To sign a message, the sender uses their private key to generate a unique cryptographic hash of the message. [75].

Confidentiality and Authentication: Asymmetric key cryptography provides confidentiality of data through encryption and authentication through digital signatures, ensuring that messages are securely transmitted and authenticated [62].

Key Distribution: Asymmetric key cryptography simplifies key distribution, as each user or entity only needs to distribute their public key widely. Private keys are kept secret and not shared.

- **Several widely used asymmetric key encryption algorithms includes the following:**

RSA (Rivest-Shamir-Adleman): One of the earliest used public key encryption method. It is used for secure communication, digital signatures, and key exchange protocols [73].

ECC: It is a modern and efficient encryption algorithm, offering similar security to RSA but with shorter key lengths, making it used for resource-constrained environments devices [76].

DSA (Digital Signature Algorithm): It is a widely used algorithm for digital signatures and authentication. Asymmetric key cryptography is well-suited for applications that require secure key exchange; secure communication between parties who have not previously shared a secret key, and authentication of messages and data integrity. Its ability to provide encryption and digital signatures without the need for pre-shared secret keys makes it a fundamental building block of modern cyber security [68].

Hash Functions: Hash functions are a fundamental concept in cryptography and information security. They are mathematical algorithms that take an input (also known as a message or data) of any length and produce a fixed-size output, which is typically a sequence of characters of fixed length called the hash value or hash digest [77].

The key properties of hash functions in cryptography are as follows:

- **Deterministic**: For the same input, a hash function will always produce the same hash value. This property is crucial for ensuring consistency in cryptographic operations.
- **Fixed Output Size**: Hash functions produce hash values of a fixed length, regardless of the size of the input data. Common hash lengths include 128, 160, 256, 384, and 512 bits [72].

- **Pre-image Resistance**: It should be computationally infeasible to reverse a hash function and retrieve the original input value from its hash value & it is called "wayness".
- **Avalanche Effect**: A small change in the input data should produce a significantly different hash value. It ensures that even minor alterations to the input result in entirely different hash outputs [78].

Various purposes of using Hash Functions for security are given below:

- **Data Integrity**: Hash functions are used to verify the integrity of data. We have to calculate the hash value of the original & receiver side [79]. One can determine if the data has been altered or tampered with during transmission or storage.
- **Digital Signatures**: Hash functions are a crucial component of digital signatures. In this context, value of a message is signed using the key of signer, providing data authenticity and non-repudiation [80].
- **Password Storage**: Hash functions are used to securely store user passwords in databases. Rather than storing the actual passwords, systems store their hash values of the original passwords. During authentication, the hash of the entered password is compared with the stored hash to verify the user's credentials [81].
- **Message Authentication Codes (MACs)**: Hash functions are used in MACs to ensure integrity & authenticity in secure communication protocols [82].
- **Block chain Technology**: Hash functions play a central role in block chain technology, where blocks of data are hashed to create a chain, ensuring data integrity and tamper resistance [83].

Frequently used hash functions include MD5, SHA-1, SHA-256, and SHA-3. It is essential to use modern and secure hash functions, as older ones, such as MD5 and SHA-1, have vulnerabilities and are no longer recommended for security-sensitive applications.

- **Advantages of Cryptography:**

Data Privacy: Cryptography ensures that only authorized parties can access and understand encrypted data, providing a high level of data privacy [12].

Data Integrity: Cryptographic techniques can detect unauthorized changes or tampering of data, ensuring data integrity [79].

Authentication: Cryptography helps verify the authenticity of messages and the identity of the communicating parties.

Secure Communication: It enables secure communication over insecure channels, protecting data from eavesdropping and unauthorized interception.

Digital Signatures: Cryptography allows the creation of digital signatures, ensuring the non-repudiation of messages or transactions [80].

- **Disadvantages of Cryptography:**

Key Management: In symmetric cryptography, managing and securely distributing the secret keys can be challenging, especially in large-scale systems.

Performance Overhead: Strong encryption algorithms can be computationally intensive, leading to a performance overhead in resource-constrained systems.

Key Compromise: If a secret key is compromised, all data encrypted with that key becomes vulnerable [84].

- **Use and application of Cryptography**:

Cryptography has numerous applications across various domains, where secure communication, data protection, and authentication are essential [83]. Some of the key applications of cryptography include:

Secure Communication: Ensuring the confidentiality and integrity of communication over insecure channels, such as the internet cryptography is used. Secure protocols like SSL/TLS (Secure Sockets Layer/Transport Layer Security) enable encrypted communication between web browsers and servers, protecting sensitive data during online transactions, login sessions, and data exchanges [85].

Data Encryption: For the encryption of sensitive data at rest or in transit, making it unreadable to unauthorized users. Encrypted data is protected from unauthorized access, theft, and tampering [68]. Disk encryption and file-level encryption are common applications to secure data on storage devices.

Digital Signatures: Cryptography enables the creation and verification of digital signatures, which provide the authenticity and integrity of digital documents, messages, and software. Digital

signatures are used in electronic documents, emails, and software updates [80].

Password Protection: Cryptographic hash functions are employed to securely store user passwords in databases. Hashing transforms the password into a fixed-length string, ensuring that even if the hashed value is compromised, the original password remains undisclosed [81].

Virtual Private Networks (VPNs): Cryptography is a fundamental component of VPNs, which create encrypted tunnels to secure data transmission between remote users and private networks. VPNs are commonly used to enhance security and privacy when accessing the internet from public or untrusted networks [86].

Wireless Security: Cryptography is essential in securing wireless networks, such as Wi-Fi, using protocols like WPA2 (Wi-Fi Protected Access II) to encrypt data and prevent unauthorized access to the network [87].

Financial Transactions: Cryptography is used to secure online financial transactions, such as credit card payments and electronic fund transfers, protecting sensitive financial information during data exchange.

Secure Messaging and Email: End-to-end encryption in messaging apps and secure email services use cryptography to ensure that only secured recipients can read the messages, providing strong privacy and protection against eavesdropping [88].

Block chain and Crypto currencies: Cryptography is a core component of block chain technology, ensuring the security and integrity of transactions in crypto currencies like Bit coin and Ethereum. Hash functions and digital signatures are used to validate and secure blocks of data in the block chain [4].

Secure Software and Firmware Updates: Cryptographic signatures and hash verification are employed to provide the authenticity & integrity of software and firmware updates. This prevents malicious code injection and ensures users are installing genuine updates [89].

Digital Rights Management (DRM): Cryptography is used in DRM systems to protect digital content from unauthorized copying, distribution, and access [90].

Secure Identity and Access Management: Cryptography is applied in secure authentication methods, such as smart cards and biometric systems, to ensure only authorized person can access sensitive resources [91].

These applications demonstrate the critical role of cryptography in safeguarding sensitive information, protecting data privacy, and enabling secure communication and transactions in our digital world.

- **Future of Cryptography**:

The future of cryptography is driven by technological advancements, emerging threats, and the need for more secure and efficient encryption methods. Several trends and developments are shaping the future of cryptography:

Quantum-Safe Cryptography: The emergence of powerful quantum computers poses a potential threat to current cryptographic methods. Quantum-safe or post-quantum cryptography aims to develop encryption algorithms that can withstand attacks from quantum computers, ensuring data security in the quantum era [66].

Multi-Party Computation: It allows multiple persons to jointly calculate a function using individual data without revealing individual inputs. This technology has applications in secure data sharing, collaborative machine learning, and privacy-preserving computations [92].

Zero-Knowledge Proofs (ZKPs): It allows one party to prove the validity of a statement to another party without sharing any information. ZKPs have implications in authentication, identity management, and digital privacy [93].

Fully Homo morphic Encryption (FHE): FHE is an advanced encryption technique that enables computation on encrypted data for any function without the need for decryption [94]. Although still in the research phase, FHE has potential applications in secure cloud computing and data privacy.

Post-Quantum Cryptography Standardization: Standardization efforts are underway to select quantum-resistant cryptographic algorithms and protocols for widespread adoption to ensure data security in the quantum era [95].

Privacy-Enhancing Technologies: Technologies that enhance privacy, including secure multiparty computation, differential confidentiality and

machine learning with privacy preservation will continue to evolve to address growing privacy concerns in data-driven applications [96].

Block chain and Crypto currencies: Cryptography is a fundamental component of block chain technology, ensuring the security and integrity of transactions in crypto currencies and decentralized applications. Improvements in block chain protocols may bring advancements in cryptographic techniques [4].

Hardware-Based Security: The integration of cryptographic functions into hardware devices (e.g., secure hardware modules and trusted execution environments) will enhance security by providing tamper-resistant and isolated environments for cryptographic operations [97].

Secure Internet of Things (IoT): As IoT devices become more pervasive, cryptographic techniques will play a crucial role in securing communications, authenticating devices, and protecting sensitive data in IoT ecosystems [98].

Privacy-Preserving AI: Research in privacy-preserving machine learning and secure AI will enable data collaboration while preserving individual data privacy and preventing unauthorized access to sensitive AI models [99].

V. Literature Review of Papers

We have reviewed some papers from 2020 to 2022 to analyze the different parameters and techniques used in security and privacy to enhance security as well as efficiency and other concepts in a proper method of encryption/decryption or any other.

Some papers are giving a novel approach to increase the integrity and confidentiality or some are working on the speed of the data uploading and downloading, etc. The summarization of their advantages is given below:

Sr. No.	Authors	Years	Techniques Purposed	Advantages
1.	Kwame Opuni-Boachie Obour Agyekum , Qi Xia , Emmanuel Boateng Sifah , Christian Nii Aflah Cobblah , Hu Xia , and Jianbin Gao[74]	2022	Re-encryption method in cloud environment to secure data.	Achieves Data Confidentiality, Security & Integrity.
2	Sara Quach & Park Thaichon & Kelly D. Martin & Scott Weaven & Robert W. Palmatier[102]	2022	Data monetization and data Sharing terms used for research in different four firms.	The different results in different firms are produced.
3.	Sanjeev Kumar, Garima Karnani, Madhu Sharma Gaur, Anju Mishra	2021	DSA and RSA algorithms are together used for providing the security.	Less time consuming when uploading and downloading data with high security is provided.
4.	K.Pavani, P.Sriramya[72]	2021	RSA algorithm with different four key are used.	High speed and low complexities are achieved in this algorithm.
5.	Abdelrahman Altigani , Shafaatunnur Hasan , Bazara Barry , (Member, Ieee), Shiraz Naserelden , Muawia A. Elsadig , And Huwaida T. Elshous[104]	2021	A polymorphic variant of the AES is used in this proposed method.	The final results pass through all STS tests and provide the better results.
6.	Shreya Dey, Ashraf Hossain[105]	2020	DiffieHellman (DH) is used with the different session keys in this proposed method.	Technique is given a strong security analyzer.
7.	Ahmed A. Abd El-Latif , Bassem Abd-El-Atty , Wojciech Mazurczyk , Senior Member, IEEE, Carol Fung, and Salvador E. Venegas-Andraca[68]	2020	S-box using 5g iot in a video file in quantum manner.	Security and efficiency is enhanced using this algorithm.
8.	OSAMA A. KHASHAN[100]	2020	RE encryption method for fog to things computing using light weighted symmetric & Asymmetric algorithm.	Results light weighted with security and efficiency.
9.	Sabyasachi Pramanik, Debabrata	2020	Cryptography blended with	Concept of two level

	Samanta, Soumi Dutta, Ramkrishna Ghosh, Mangesh Ghonge, Digvijay Pandey[101]		steganography in 2 layer's protection by using RSA in first and LSB techniques in second part.	securities achieved.
10.	Md. Alamgir Hossain a and Md. Abdullah Al Hasan b[103]	2020	Hybrid verification technique based upon biometric and encryption system.	To achieve authentication by checking the unapproved clients.

VI. CONCLUSION

Data security is a critical aspect of modern information technology and business practices. It is essential for protecting sensitive information, ensuring business continuity, complying with regulations, and maintaining customer trust. By employing encryption, access controls, firewalls, and other security measures, organizations can strengthen their data security posture and defend against evolving cyber threats. Data security is an ongoing process that requires continuous monitoring, updates to security measures, and employee training to stay ahead of potential vulnerabilities and attacks. By investing in robust data security measures, organizations can effectively safeguard their data assets and maintain a competitive advantage in the digital age.

Data privacy is a complex and multifaceted issue that requires careful consideration from all stakeholders involved. Legal frameworks, technical solutions, and ethical considerations must be integrated to ensure that individuals' privacy rights are protected without hindering innovation and progress. As technology continues to advance, graduate-level professionals must stay informed about the evolving challenges and solutions in data privacy to build a more secure and privacy-conscious digital future.

The future of cryptography will be characterized by advancements in quantum-resistant encryption, secure computation techniques, and privacy-preserving technologies to address evolving security challenges in an increasingly digital and interconnected world. The ongoing research and standardization efforts will shape the cryptographic landscape to ensure robust and secure communication and data protection in the years to come.

REFERENCES

1. T. Wang, Q. Yang, X. Shen, T. R. Gadekallu, W. Wang, and K. Dev, 'A Privacy-Enhanced Retrieval Technology for the Cloud-Assisted Internet of Things', IEEE Trans. Ind. Inf., vol. 18, no. 7, pp. 4981–4989, Jul. 2022, doi: 10.1109/TII.2021.3103547.
2. P. Goel, R. Patel, D. Garg, and A. Ganatra, 'A Review on Big Data: Privacy and Security Challenges', in 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India: IEEE, May 2021, pp. 705–709. doi: 10.1109/ICSPC51351.2021.9451749.
3. Z. He, T. Zhang, and R. B. Lee, 'Attacking and Protecting Data Privacy in Edge–Cloud Collaborative Inference Systems', IEEE Internet Things J., vol. 8, no. 12, pp. 9706–9716, Jun. 2021, doi: 10.1109/JIOT.2020.3022358.
4. H. Xu, Q. He, X. Li, B. Jiang, and K. Qin, 'BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control', IEEE Access, vol. 8, pp. 87552–87561, 2020, doi: 10.1109/ACCESS.2020.2992649.
5. T. Jabeen, H. Ashraf, A. Khatoon, S. S. Band, and A. Mosavi, 'A Lightweight Genetic Based Algorithm for Data Security in Wireless Body Area Networks', IEEE Access, vol. 8, pp. 183460–183469, 2020, doi: 10.1109/ACCESS.2020.3028686.
6. T. Quintel, 'Data protection rules applicable to Financial Intelligence Units: still no clarity in sight', ERA Forum, vol. 23, no. 1, pp. 53–74, May 2022, doi: 10.1007/s12027-021-00697-z.
7. H. Mathur and Z. Alam, 'Analysis In Symmetric And Asymmetric Cryptology Algorithm', vol. 4, no. 1, 2015.
8. R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, 'A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions', IEEE Commun. Surv. Tutorials, vol. 22, no. 1, pp. 196–248, 2020, doi: 10.1109/COMST.2019.2933899.
9. P. Yang, N. Xiong, and J. Ren, 'Data Security and Privacy Protection for Cloud Storage: A Survey', IEEE Access, vol. 8, pp. 131723–131740, 2020, doi: 10.1109/ACCESS.2020.3009876.
10. J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, 'Privacy-Preserving Solutions for Blockchain: Review and Challenges', IEEE

Access, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.
11. M. Whaiduzzaman et al., 'A Privacy-Preserving Mobile and Fog Computing Framework to Trace and Prevent COVID-19 Community Transmission', IEEE J. Biomed. Health Inform., vol. 24, no. 12, pp. 3564–3575, Dec. 2020, doi: 10.1109/JBHI.2020.3026060.
12. M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, 'Smart Meter Data Privacy: A Survey', IEEE Commun. Surv. Tutorials, vol. 19, no. 4, pp. 2820–2835, 2017, doi: 10.1109/COMST.2017.2720195.
13. H. Hu, J. Xu, C. Ren, and B. Choi, 'Processing private queries over untrusted data cloud through privacy homomorphism', in 2011 IEEE 27th International Conference on Data Engineering, Hannover, Germany: IEEE, Apr. 2011, pp. 601–612. doi: 10.1109/ICDE.2011.5767862.
14. X. Huang and X. Du, 'Achieving big data privacy via hybrid cloud', in 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada: IEEE, Apr. 2014, pp. 512–517. doi: 10.1109/INFCOMW.2014.6849284.
15. P. Sirohi and A. Agarwal, 'Cloud computing data storage security framework relating to data integrity, privacy and trust', in 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India: IEEE, Sep. 2015, pp. 115–118. doi: 10.1109/NGCT.2015.7375094.
16. M. S. Hossain et al., 'Impact of Next-Generation Mobile Technologies on IoT-Cloud Convergence', IEEE Commun. Mag., vol. 55, no. 1, pp. 18–19, Jan. 2017, doi: 10.1109/MCOM.2017.7823332.
17. X. Chen, X. Wang, and K. Yang, 'Asynchronous Blockchain-based Privacy-preserving Training Framework for Disease Diagnosis', in 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA: IEEE, Dec. 2019, pp. 5469–5473. doi: 10.1109/BigData47090.2019.9006173.
18. J. Komljenovic, 'The future of value in digitalised higher education: why data privacy should not be our biggest concern', High Educ, vol. 83, no. 1, pp. 119–135, Jan. 2022, doi: 10.1007/s10734-020-00639-7.
19. A. Saini, K. Joshi, and S. Allawadhi, 'A Review On Video Steganography Techniques', International Journal of Advanced Research in Computer Science, 2017.
20. F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, 'DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL', Information & Management, vol. 58, no. 1, p. 103392, Jan. 2021, doi: 10.1016/j.im.2020.103392.
21. S. A. Shah, D. Z. Seker, S. Hameed, and D. Draheim, 'The Rising Role of Big Data Analytics and IoT in Disaster Management: Recent Advances, Taxonomy and Prospects', IEEE Access, vol. 7, pp. 54595–54614, 2019, doi: 10.1109/ACCESS.2019.2913340.
22. K. Kiela et al., 'Review of V2X–IoT Standards and Frameworks for ITS Applications', Applied Sciences, vol. 10, no. 12, p. 4314, Jun. 2020, doi: 10.3390/app10124314.
23. N. S. Mullah and W. M. N. W. Zainon, 'Advances in Machine Learning Algorithms for Hate Speech Detection in Social Media: A Review', IEEE Access, vol. 9, pp. 88364–88376, 2021, doi: 10.1109/ACCESS.2021.3089515.
24. X. Liu, J. Liu, S. Zhu, W. Wang, and X. Zhang, 'Privacy Risk Analysis and Mitigation of Analytics Libraries in the Android Ecosystem', IEEE Trans. on Mobile Comput., vol. 19, no. 5, pp. 1184–1199, May 2020, doi: 10.1109/TMC.2019.2903186.
25. X. Zheng and Z. Cai, 'Privacy-Preserved Data Sharing Towards Multiple Parties in Industrial IoTs', IEEE J. Select. Areas Commun., vol. 38, no. 5, pp. 968–979, May 2020, doi: 10.1109/JSAC.2020.2980802.
26. 'THE LONG-TERM COSTS OF GOVERNMENT SURVEILLANCE: INSIGHTS FROM STASI SPYING IN EAST GERMANY', Journal of the European Economic Association.
27. H. Jin, Y. Luo, P. Li, and J. Mathew, 'A Review of Secure and Privacy-Preserving Medical Data Sharing', IEEE Access, vol. 7, pp. 61656–61669, 2019, doi: 10.1109/ACCESS.2019.2916503.
28. M. Barreto, C. Victor, C. Hammond, A. Eccles, M. T. Richins, and P. Qualter, 'Loneliness around the world: Age, gender, and cultural differences in loneliness', Personality and Individual Differences, vol. 169, p. 110066, Feb. 2021, doi: 10.1016/j.paid.2020.110066.
29. J. Zhao, Y. Chen, and W. Zhang, 'Differential Privacy Preservation in Deep Learning: Challenges, Opportunities and

Solutions', IEEE Access, vol. 7, pp. 48901–48911, 2019, doi: 10.1109/ACCESS.2019.2909559.
30. I. Goldberg, D. Wagner, and E. Brewer, 'Privacy-enhancing technologies for the Internet'.
31. C. Lima, 'Developing Open and Interoperable DLT\/Blockchain Standards [Standards]', Computer, vol. 51, no. 11, pp. 106–111, Nov. 2018, doi: 10.1109/MC.2018.2876184.
32. J. Tse, D. E. Schrader, D. Ghosh, T. Liao, and D. Lundie, 'A bibliometric analysis of privacy and ethics in IEEE Security and Privacy', Ethics Inf Technol, vol. 17, no. 2, pp. 153–163, Jun. 2015, doi: 10.1007/s10676-015-9369-6.
33. J. Bringer, H. Chabanne, and A. Patey, 'Privacy-Preserving Biometric Identification Using Secure Multiparty Computation: An Overview and Recent Trends', IEEE Signal Process. Mag., vol. 30, no. 2, pp. 42–52, Mar. 2013, doi: 10.1109/MSP.2012.2230218.
34. B. C. Stahl and D. Wright, 'Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation', IEEE Secur. Privacy, vol. 16, no. 3, pp. 26–33, May 2018, doi: 10.1109/MSP.2018.2701164.
35. N. Naik and P. Jenkins, 'Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology', in 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, GB: IEEE, Aug. 2020, pp. 90–95. doi: 10.1109/MobileCloud48802.2020.00021.
36. P. Zhou, K. Wang, L. Guo, S. Gong, and B. Zheng, 'A Privacy-Preserving Distributed Contextual Federated Online Learning Framework with Big Data Support in Social Recommender Systems', IEEE Trans. Knowl. Data Eng., pp. 1–1, 2019, doi: 10.1109/TKDE.2019.2936565.
37. S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, 'PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management', IEEE Access, vol. 7, pp. 6117–6128, 2019, doi: 10.1109/ACCESS.2018.2889898.
38. J. Wang et al., 'Quantum-safe cryptography: crossroads of coding theory and cryptography', Sci. China Inf. Sci., vol. 65, no. 1, p. 111301, Jan. 2022, doi: 10.1007/s11432-021-3354-7.
39. R. Eitel-Porter, 'Beyond the promise: implementing ethical AI', AI Ethics, vol. 1, no. 1, pp. 73–80, Feb. 2021, doi: 10.1007/s43681-020-00011-6.
40. A. Saini, K. Joshi, K. Sharma, and R. Nandal, 'An Analysis of LSB Technique in Video Steganography using PSNR and MSE', International Journal of Advanced Research in Computer Science, 2017.
41. A. Bates and W. U. Hassan, 'Can Data Provenance Put an End to the Data Breach?', IEEE Secur. Privacy, vol. 17, no. 4, pp. 88–93, Jul. 2019, doi: 10.1109/MSEC.2019.2913693.
42. M. M. H. Onik, C.-S. Kim, and J. Yang, 'Personal Data Privacy Challenges of the Fourth Industrial Revolution', in 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South): IEEE, Feb. 2019, pp. 635–638. doi: 10.23919/ICACT.2019.8701932.
43. D. Moongilan, '5G Internet of Things (IOT) Near and Far-Fields and Regulatory Compliance Intricacies', in 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland: IEEE, Apr. 2019, pp. 894–898. doi: 10.1109/WF-IoT.2019.8767334.
44. S. Sayeed and H. Marco-Gisbert, 'Smart Contract: Attacks and Protections', vol. 8, 2020.
45. D. Zhang, L. Yao, K. Chen, G. Long, and S. Wang, 'Collective Protection: Preventing Sensitive Inferences via Integrative Transformation', in 2019 IEEE International Conference on Data Mining (ICDM), Beijing, China: IEEE, Nov. 2019, pp. 1498–1503. doi: 10.1109/ICDM.2019.00197.
46. M. Barati, O. Rana, I. Petri, and G. Theodorakopoulos, 'GDPR Compliance Verification in Internet of Things', IEEE Access, vol. 8, pp. 119697–119709, 2020, doi: 10.1109/ACCESS.2020.3005509.
47. Y. Fang, Y. Guo, C. Huang, and L. Liu, 'Analyzing and Identifying Data Breaches in Underground Forums', IEEE Access, vol. 7, pp. 48770–48777, 2019, doi: 10.1109/ACCESS.2019.2910229.
48. A. Chakraborty, A. Mondai, and A. Srivastava, 'Hardware-Assisted Intellectual Property Protection of Deep Learning Models', in 2020 57th ACM/IEEE Design Automation Conference (DAC), San Francisco, CA, USA: IEEE, Jul. 2020, pp. 1–6. doi: 10.1109/DAC18072.2020.9218651.

49. J. Priyanka and M. Ramakrishna, 'Performance Analysis of Attribute based Encryption and Cloud Health data Security', in 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India: IEEE, May 2020, pp. 989–994. doi: 10.1109/ICICCS48265.2020.9120894.
50. B. Ali, M. A. Gregory, and S. Li, 'Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review', IEEE Access, vol. 9, pp. 18706–18721, 2021, doi: 10.1109/ACCESS.2021.3053233.
51. A. K. Pandey et al., 'Key Issues in Healthcare Data Integrity: Analysis and Recommendations', vol. 8, 2020.
52. W. Fang, 'Digital signature scheme for information non-repudiation in blockchain: a state of the art review', 2020.
53. C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, 'AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud', IEEE Access, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.
54. M. Joshi, S. Budhani, N. Tewari, and S. Prakash, 'Analytical Review of Data Security in Cloud Computing', in 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom: IEEE, Apr. 2021, pp. 362–366. doi: 10.1109/ICIEM51511.2021.9445355.
55. L.-X. Yang, K. Huang, X. Yang, Y. Zhang, Y. Xiang, and Y. Y. Tang, 'Defense Against Advanced Persistent Threat Through Data Backup and Recovery', IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2001–2013, Jul. 2021, doi: 10.1109/TNSE.2020.3040247.
56. F. Shahid, H. Ashraf, A. Ghani, S. A. K. Ghayyur, S. Shamshirband, and E. Salwana, 'PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud', IEEE Access, vol. 8, pp. 118285–118298, 2020, doi: 10.1109/ACCESS.2020.3004433.
57. R. K. Jamra, B. Anggorojati, Kautsarina, D. I. Sensuse, and R. R. Suryono, 'Systematic Review of Issues and Solutions for Security in E-commerce', in 2020 International Conference on Electrical Engineering and Informatics (ICELTICs), Aceh, Indonesia: IEEE, Oct. 2020, pp. 1–5. doi: 10.1109/ICELTICs50595.2020.9315437.
58. N. Suresh, G. L. Sanders, and M. J. Braunscheidel, 'Business Continuity Management for Supply Chains Facing Catastrophic Events', IEEE Eng. Manag. Rev., vol. 48, no. 3, pp. 129–138, Sep. 2020, doi: 10.1109/EMR.2020.3005506.
59. N. Lin, X. Chen, H. Lu, and X. Li, 'Chaotic Weights: A Novel Approach to Protect Intellectual Property of Deep Neural Networks', IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol. 40, no. 7, pp. 1327–1339, Jul. 2021, doi: 10.1109/TCAD.2020.3018403.
60. A. Saini, K. Joshi, and S. Allawadhi, 'A Review On Video Steganography Techniques', International Journal of Advanced Research in Computer Science, 2017.
61. P. Rastegari, 'On the Security of Some Recently Proposed Certificateless Signcryption Schemes', in 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran: IEEE, Sep. 2020, pp. 95–100. doi: 10.1109/ISCISC51277.2020.9261917.
62. A. M. Qadir and N. Varol, 'A Review Paper on Cryptography', in 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal: IEEE, Jun. 2019, pp. 1–6. doi: 10.1109/ISDFS.2019.8757514.
63. M. T. Gençoğlu, 'Importance of Cryptography in Information Security'.
64. L. Voleti, R. M. Balajee, S. K. Vallepu, K. Bayoju, and D. Srinivas, 'A Secure Image Steganography Using Improved Lsb Technique And Vigenere Cipher Algorithm', in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India: IEEE, Mar. 2021, pp. 1005–1010. doi: 10.1109/ICAIS50930.2021.9395794.
65. J. Kaur, S. Lamba, and P. Saini, 'Advanced Encryption Standard: Attacks and Current Research Trends', in 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India: IEEE, Mar. 2021, pp. 112–116. doi: 10.1109/ICACITE51222.2021.9404716.
66. T. M. Fernandez-Carames and P. Fraga-Lamas, 'Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks', IEEE Access, vol. 8, pp. 21091–21116, 2020, doi: 10.1109/ACCESS.2020.2968985.
67. M. Bansal, S. Gupta, and S. Mathur, 'Comparison of ECC and RSA Algorithm with DNA Encoding for IoT Security', in 2021 6th International Conference on

Inventive Computation Technologies (ICICT), Coimbatore, India: IEEE, Jan. 2021, pp. 1340–1343. doi: 10.1109/ICICT50816.2021.9358591.

68. A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, 'Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario', IEEE Trans. Netw. Serv. Manage., vol. 17, no. 1, pp. 118–131, Mar. 2020, doi: 10.1109/TNSM.2020.2969863.
69. S. Chen, W. Hu, and Z. Li, 'High Performance Data Encryption with AES Implementation on FPGA', in 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA: IEEE, May 2019, pp. 149–153. doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00036.
70. S. Dey and A. Hossain, 'Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography', IEEE Sens. Lett., vol. 3, no. 4, pp. 1–4, Apr. 2019, doi: 10.1109/LSENS.2019.2905020.
71. K. Sowjanya and M. Dasgupta, 'Survey of Symmetric and Asymmetric Key Management Schemes in the context of IoT based Healthcare System', in 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India: IEEE, Jan. 2020, pp. 283–288. doi: 10.1109/ICPC2T48082.2020.9071446.
72. K. Pavani and P. Sriramya, 'Enhancing Public Key Cryptography using RSA, RSA-CRT and N-Prime RSA with Multiple Keys', in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India: IEEE, Feb. 2021, pp. 1–6. doi: 10.1109/ICICV50876.2021.9388621.
73. A. Hamza and B. Kumar, 'A Review Paper on DES, AES, RSA Encryption Standards', in 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), Moradabad, India: IEEE, Dec. 2020, pp. 333–338. doi: 10.1109/SMART50582.2020.9336800.
74. K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, 'A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain', IEEE Systems Journal, vol. 16, no. 1, pp. 1685–1696, Mar. 2022, doi: 10.1109/JSYST.2021.3076759.
75. M. Bisheh-Niasar, R. Azarderakhsh, and M. Mozaffari-Kermani, 'Cryptographic Accelerators for Digital Signature Based on Ed25519', IEEE Trans. VLSI Syst., vol. 29, no. 7, pp. 1297–1305, Jul. 2021, doi: 10.1109/TVLSI.2021.3077885.
76. M. A. Mehrabi, C. Doche, and A. Jolfaei, 'Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module', IEEE Trans. Comput., vol. 69, no. 11, pp. 1707–1718, Nov. 2020, doi: 10.1109/TC.2020.3013266.
77. A. K. Sharma and S. K. Mittal, 'Cryptography & Network Security Hash Function Applications, Attacks and Advances: A Review', in 2019 Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India: IEEE, Jan. 2019, pp. 177–188. doi: 10.1109/ICISC44355.2019.9036448.
78. S. D. Sanap and V. More, 'Performance Analysis of Encryption Techniques Based on Avalanche effect and Strict Avalanche Criterion', in 2021 3rd International Conference on Signal Processing and Communication (ICPSC), Coimbatore, India: IEEE, May 2021, pp. 676–679. doi: 10.1109/ICSPC51351.2021.9451784.
79. V. Fomichev, D. Bobrovskiy, A. Koreneva, T. Nabiev, and D. Zadorozhny, 'Data integrity algorithm based on additive generators and hash function', J Comput Virol Hack Tech, vol. 18, no. 1, pp. 31–41, Mar. 2022, doi: 10.1007/s11416-021-00405-y.
80. W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, 'Digital signature scheme for information non-repudiation in blockchain: a state of the art review', J Wireless Com Network, vol. 2020, no. 1, p. 56, Dec. 2020, doi: 10.1186/s13638-020-01665-w.
81. J. Polpong and P. Wuttidittachotti, 'Authentication and password storing improvement using SXR algorithm with a hash function', IJECE, vol. 10, no. 6, p. 6582, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6582-6591.
82. J. Ali and V. Dyo, 'Practical Hash-based Anonymity for MAC Addresses', in Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, 2020, pp. 572–579. doi: 10.5220/0009825105720579.

83. S. Abed, R. Jaffal, B. J. Mohd, and M. Al-Shayeji, 'An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices', Cluster Comput, vol. 24, no. 4, pp. 3065–3084, Dec. 2021, doi: 10.1007/s10586-021-03324-1.
84. A. Hadipour and R. Afifi, 'Advantages and disadvantages of using cryptography in steganography', in 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran: IEEE, Sep. 2020, pp. 88–94. doi: 10.1109/ISCISC51277.2020.9261921.
85. L. Fang, H. Zhang, M. Li, C. Ge, L. Liu, and Z. Liu, 'A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City', IEEE Internet Things J., vol. 7, no. 9, pp. 7982–7990, Sep. 2020, doi: 10.1109/JIOT.2020.2996664.
86. T. Lackorzynski, S. Kopsell, and T. Strufe, 'A Comparative Study on Virtual Private Networks for Future Industrial Communication Systems', in 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS), Sundsvall, Sweden: IEEE, May 2019, pp. 1–8. doi: 10.1109/WFCS.2019.8758010.
87. Ompal, V. M. Mishra, and A. Kumar, 'FPGA integrated IEEE 802.15.4 ZigBee wireless sensor nodes performance for industrial plant monitoring and automation', Nuclear Engineering and Technology, vol. 54, no. 7, pp. 2444–2452, Jul. 2022, doi: 10.1016/j.net.2022.01.011.
88. D. Zhang, L. Yao, K. Chen, G. Long, and S. Wang, 'Collective Protection: Preventing Sensitive Inferences via Integrative Transformation', in 2019 IEEE International Conference on Data Mining (ICDM), Beijing, China: IEEE, Nov. 2019, pp. 1498–1503. doi: 10.1109/ICDM.2019.00197.
89. K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli, 'Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check', IEEE Access, vol. 7, pp. 71907–71920, 2019, doi: 10.1109/ACCESS.2019.2919760.
90. Z. Yan, V. Govindaraju, Q. Zheng, and Y. Wang, 'IEEE Access Special Section Editorial: Trusted Computing', IEEE Access, vol. 8, pp. 25722–25726, 2020, doi: 10.1109/ACCESS.2020.2969768.
91. R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, 'SSIBAC: Self-Sovereign Identity Based Access Control', in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China: IEEE, Dec. 2020, pp. 1935–1943. doi: 10.1109/TrustCom50675.2020.00264.
92. H. Gao, Z. Ma, S. Luo, and Z. Wang, 'BFR-MPC: A Blockchain-Based Fair and Robust Multi-Party Computation Scheme', IEEE Access, vol. 7, pp. 110439–110450, 2019, doi: 10.1109/ACCESS.2019.2934147.
93. Z. Mahmood and J. Vacius, 'Privacy-Preserving Block-chain Framework Based on Ring Signatures (RSs) and Zero-Knowledge Proofs(ZKPs)', in 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain: IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/3ICT51146.2020.9312014.
94. W. Liang, D. Zhang, X. Lei, M. Tang, K.-C. Li, and A. Y. Zomaya, 'Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection', IEEE Trans. Emerg. Topics Comput., vol. 9, no. 3, pp. 1410–1420, Jul. 2021, doi: 10.1109/TETC.2020.2993032.
95. T. M. Fernandez-Carames, 'From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things', IEEE Internet Things J., vol. 7, no. 7, pp. 6457–6480, Jul. 2020, doi: 10.1109/JIOT.2019.2958788.
96. I. Goldberg, D. Wagner, and E. Brewer, 'Privacy-enhancing technologies for the Internet'.
97. N. Karimi, K. Basu, C.-H. Chang, and J. M. Fung, 'Hardware Security in Emerging Technologies: Vulnerabilities, Attacks, and Solutions', IEEE J. Emerg. Sel. Topics Circuits Syst., vol. 11, no. 2, pp. 223–227, Jun. 2021, doi: 10.1109/JETCAS.2021.3084498.
98. F. Alshehri and G. Muhammad, 'A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare', IEEE Access, vol. 9, pp. 3660–3678, 2021, doi: 10.1109/ACCESS.2020.3047960.
99. Q. Kong et al., 'Privacy-Preserving Aggregation for Federated Learning-Based Navigation in Vehicular Fog', IEEE Trans. Ind. Inf., vol. 17, no. 12, pp. 8453–8463, Dec. 2021, doi: 10.1109/TII.2021.3075683.
100. O. A. Khashan, 'Hybrid Lightweight Proxy Re-Encryption Scheme for Secure Fog-to-Things Environment', IEEE Access, vol. 8,

pp. 66878–66887, 2020, doi: 10.1109/ACCESS.2020.2984317.
101. S. Pramanik, D. Samanta, S. Dutta, R. Ghosh, M. Ghonge, and D. Pandey, 'Steganography using Improved LSB Approach and Asymmetric Cryptography', in 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI), Buldhana, India: IEEE, Dec. 2020, pp. 1–5. doi: 10.1109/ICATMRI51801.2020.9398408.
102. S. Quach, P. Thaichon, K. D. Martin, S. Weaven, and R. W. Palmatier, 'Digital technologies: tensions in privacy and data', J. of the Acad. Mark. Sci., vol. 50, no. 6, pp. 1299–1323, Nov. 2022, doi: 10.1007/s11747-022-00845-y.
103. Md. A. Hossain and Md. A. Al Hasan, 'Improving cloud data security through hybrid verification technique based on biometrics and encryption system', International Journal of Computers and Applications, vol. 44, no. 5, pp. 455–464, May 2022, doi: 10.1080/1206212X.2020.1809177.
104. A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, 'A Polymorphic Advanced Encryption Standard – A Novel Approach', IEEE Access, vol. 9, pp. 20191–20207, 2021, doi: 10.1109/ACCESS.2021.3051556.
105. S. Dey and A. Hossain, 'Session-Key Establishment and Authentication in a Smart Home Network Using Public Key Cryptography', IEEE Sens. Lett., vol. 3, no. 4, pp. 1–4, Apr. 2019, doi: 10.1109/LSENS.2019.2905020.