VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

A CRITICAL ANALYSIS OF INDIA'S ENCRYPTION POLICY: ALIGNING WITH GLOBAL STANDARDS

- Satendra Rajput*

Abstract

“*This research paper offers a comprehensive examination of India's encryption policy within the context of international standards and practices. Encryption, being a pivotal aspect of cybersecurity and digital privacy, demands careful scrutiny and alignment with global norms. Through an in-depth analysis, this paper aims to shed light on India's encryption regulations, their effectiveness, and their compatibility with international benchmarks. By assessing India's encryption policy through the lens of global standards, this study identifies areas for improvement and proposes strategies for ensuring alignment with the evolving landscape of encryption practices worldwide.*”

I. INTRODUCTION

Encryption is a fundamental concept in the realm of cybersecurity and information technology, serving as a cornerstone for securing sensitive data and communications.[1] At its core, encryption involves the process of converting plaintext information into ciphertext, rendering it unintelligible to unauthorized individuals or entities. This transformation relies on complex mathematical algorithms and cryptographic techniques to ensure the confidentiality, integrity, and authenticity of digital information.

The roots of encryption may be traceable back to times of antiquity when cryptography manifested in many forms. we possess evidence of cryptographic methods dating back to

* Author - Satendra Rajput, Ph.D. Research Scholar, Himachal Pradesh National Law University, Shimla

[1] Brent Waters, *Functional Encryption: Origins and Recent Developments*, Springer, Berlin, 7778 HEIDELBERG, 21, 21 - 54 (2013).

1900 BC in Egypt.[2] This evidence comes from an inscription found in the main vault of the tomb of nobleman Khnumhotep II.[3] The hieroglyphics employed exhibited variations from the conventional ones, employing a technique presently recognised as symbol substitution. Nevertheless, this was not always an encrypted message. Instead, they altered the writing style to give it a more respectable appearance.

During the year 1500 BC, a scribe from Mesopotamia employed cryptography to hide a recipe for ceramic glaze.[4] This example is the earliest documented instance of utilising encryption to concealconfidential data.However, there are other cases as well. Cryptography has been documented in nearly all significant ancient civilizations. During ancient times in India, Kautilya, also known as Chanakya, wrote a book called "Arthashastra" which detailed the allocation of tasks to spies using a method known as secret writing.[5]

The ancient Greeks employed cyphers, which are algorithms utilised for the purpose of encrypting or decrypting messages, in order to alter the content of a communication. Julius Caesar employed a kind of encryption around 100 BC to clandestinely communicate with his military commanders during times of conflict.[6] The Caesar Cypher is widely recognised as one of the most prominent applications of encryption. A substitution cypher, sometimes referred to as a simple replacement cypher, involves replacing each character of the plain text with another character to create the cypher text.[7] For instance, the letter A is transformed into D, B is transformed into E, and C is transformed into F. Can you observe the pattern of shifting each letter by 3 positions?

A new way of encryption, Known as The Vigenère Cypher originated in the 16th century. This technique employs a sequence of intertwined Caesar cyphers to encrypt alphabetical text, relying on the letters of a keyword. This phenomenon is referred to as

[2] Dwiti Pandya et. al., *Brief History of Encryption*, 131(9) INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS, 28, 29-30 (2015).

[3] GIANLUCA MINIACI, WOLFRAM GRAJETZKI (ED.), 1 THE WORLD OF MIDDLE KINGDOM EGYPT (2000-1550 BC) 55 (Golden House Publications, 2015).

[4] Dwiti Pandya et. al.,*Supra* Note 2.

[5] Kautiya'sArthashastra

[6] G. Pelosi and S. Selleri, "*Florence and a Leap in Cryptography: The Leon Battista Alberti Cypher Disk*," 2021 7th IEEE History of Electrotechnology Conference (HISTELCON), Moscow, Russian Federation, 2021, pp. 7-11

[7] Ibid.

polyalphabetic substitution.[8] Although Giovan Battista Bellaso initially described it in 1553, Blaise de Vigènere was credited with it in the 19th century. Despite its increased security compared to the Caesar cypher and its widespread implementation, the Vigènere cypher was successfully decrypted in 1863 by Friedrich Kasiski. [9]

The contemporary age of encryption started in the mid-20th century[10] with the introduction of electromechanical and electronic encryption equipment.[11] The German Enigma machine, utilised by the Axis forces in World War II, is renowned as one of the most prominent encryption systems of its day, employed to cypher military communications. The Enigma machine utilised intricate rotors and electrical circuits to encrypt communications, presenting a significant obstacle to Allied codebreakers.

After the war, cryptography underwent a significant transformation with the emergence of public-key cryptography in the 1970s.[12] This breakthrough was achieved by researchers like Whitfield Diffie, Martin Hellman, and Ralph Merkle. Public-key cryptography revolutionised encryption by introducing the notion of asymmetric encryption, which involves the use of distinct keys for encryption and decoding. This significant advancement established the basis for safe digital communication across unreliable channels, serving as the groundwork for contemporary encryption protocols like the Secure Sockets Layer (SSL) and its subsequent iteration, Transport Layer Security (TLS).

Currently, encryption is of utmost importance in protecting confidential information in several sectors such as banking, healthcare, government, and telecommunications. It provides the foundation for the security of online transactions, safeguards personal privacy, and ensures the secrecy of business interactions.[13] Due to the widespread use of digital

[8] Agung Purnomo Sidik, *Improve The Security of The Vigenère Cypher Algorithm by Modifying the Encoding Table and Key*, 10(2) INTERNATIONAL JOURNAL OF BASIC AND APPLIED SCIENCE, 42, 42-43 (2021).
[9] Ibid.
[10] Jean-Baptiste Doumenjou, *The Evolution of Cryptography in Modern History*, TRARFIKLABS (Nov. 8, 2022). Available at https://traefik.io/blog/the-evolution-of-cryptography-in-modern-history/.
[11] Ibid
[12] Sanjay Kumar Pal and Shubham Mishra, *Revolutionary Change in Cryptography*, 9(2) INVERTIS JOURNAL OF RENEWABLE ENERGY, 43, 47 – 49 (2019).
[13] Brent Waters, *Supra* Note 01 at 33-40.

technology and the increased risk of cyberattacks, encryption is constantly developing to address the needs of a more linked global society.[14]

In accordance with IT Rules, 2000 encryption is elucidated as follows: "*The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).*"[15] This definition underscores the pivotal role encryption plays in securing digital information, whether in transit or storage. Cryptographic techniques serve as the bedrock for managing access to critical and sensitive data across the internet, thereby fortifying the integrity and confidentiality of digital communications and assets.

Within the domain of network protocols, a relevant instance that highlights the importance of encryption is the distinction between HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure). HTTPS is a more secure version of HTTP that incorporates Transport Layer Security (TLS), formerly known as Secure Sockets Layer (SSL), to encrypt HTTP data during transmission. Therefore, HTTPS outperforms HTTP in terms of security effectiveness. It is evident that a website using the HTTP protocol will display "http://" in its URL, whereas a website using the HTTPS protocol will show "https://". This evaluation is essential for determining the encryption state of online platforms and highlights the crucial function of encryption in strengthening digital security standards.

III. PROCESS OF CRYPTOGRAPHY

Cryptography is the field of study and application that focuses on protecting the transmission of information by employing cryptographic methods and procedures. Cryptography is the practice of encrypting information in a manner that renders it incomprehensible to anybody without the necessary decryption key. Encryption is a core component of cryptography, in which plain data is converted into coded data using an encryption method and a confidential key. There are following steps in cryptography: –

1. Sender

[14] Amit Sahai and Brent Waters,*Fuzzy identity-based encryption*. IN EUROCRYPT, 457, 457–473, (2005).
[15] The Information Technology (Certifying Authorities) Rules, 2000.

2. Receiver

3. Cryptography key

1. Sender: A person or user who sent text or other material, called the sender.

2. Receiver:A person or user who received text/messages or other material sent by the sender called the receiver.

3: Cryptography Keys: In cryptography, keys are essential components used in encryption and decryption processes to secure digital information. They play a pivotal role in determining how data is transformed from plaintext to ciphertext (encryption) and back again (decryption). Cryptography keys come in different forms and are utilized in various encryption algorithms to provide security and confidentiality. There are the following types of cryptographic keys:

i. Symmetric Keys:

Symmetric keys, also known as secret keys or private keys, are identical keys shared between communicating parties to encrypt and decrypt data.[16]IT Rules, 20004 defined public key cryptography as "*A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.*"

[16]S. Picek and M. Golub, "On evolutionary computation methods in cryptography," 2011 Proceedings of the 34th International Convention MIPRO, Opatija, Croatia, 2011, pp. 1496-1501 at 1497.

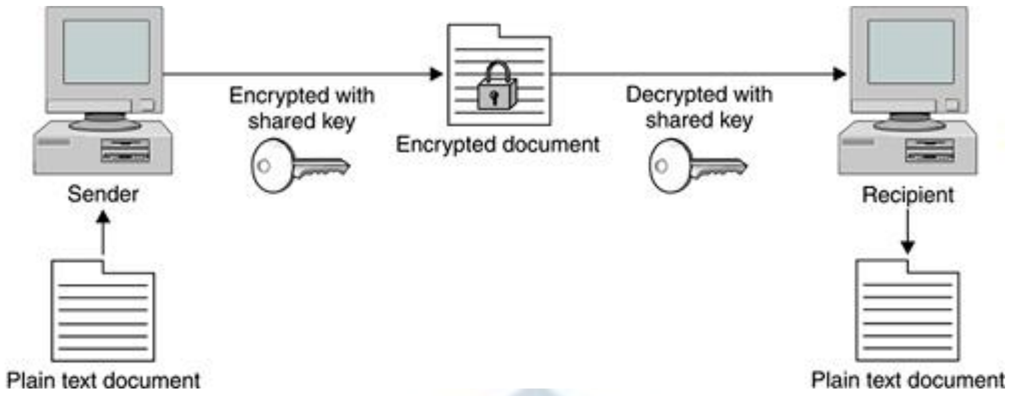

Image: Symmetric Encryption[17]

Symmetric-key cryptography employs a single key for both the encryption and decryption operations. Consequently, it is necessary for both the sender and recipient to hold an identical key in order to ensure the security of their connection. Symmetric-key methods, such as AES and DES, are highly efficient for encrypting huge volumes of data because of their simplicity and speed.[18]

For example,

A. Payment applications, such as card transactions, require the protection of personally identifiable information (PII) to avoid identity theft or fraudulent charges.
B. Verifications to authenticate the identity of the text source.

ii. Asymmetric Keys or Private Keys:

Asymmetric keys, also known as public-private key pairs, involve the use of two distinct keys: a public key and a private key.[19] Asymmetric-key cryptography enables secure communication between parties without the need for a pre-shared secret key.[20]

[17] Image Source: http://books.gigatux.nl/mirror/securitytools/ddu/ch09lev1sec1.html.
[18] B. SCHNEIER, "APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, 65-88 (2nd Edt., Wiley; USA, 1996).
[19] M. B. Yassein Et. Al, *Comprehensive study of symmetric key and asymmetric key encryption algorithms*,2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 2017, pp. 1-7 at 3 – 5.
[20] *Ibid.*

In Schedule V of the IT Rules, 20003 define public key as "*PUBLIC KEY is the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.*"[21]

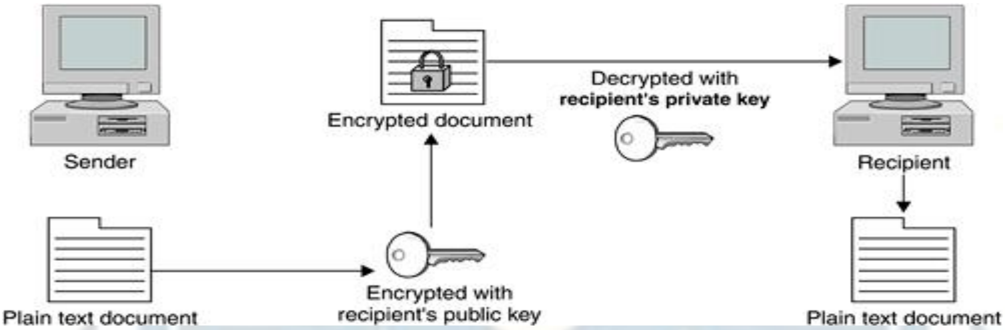
Sender
Encrypted document
Decrypted with recipient's private key
Recipient
Plain text document
Encrypted with recipient's public key
Plain text document

Image: Asymmetric Encryption[22]

The public key, which is extensively disseminated, is employed for the purpose of encryption, whilst the private key, maintained in secrecy by the administrator, is utilised for the process of decoding. On the other hand, material that is encoded using the private key can only be decoded using the matching public key. This allows for the creation of digital signatures and ensures that the sender cannot deny their involvement. Two widely used asymmetric encryption methods are RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC). In asymmetric cryptography, data is encrypted using one key and decoded using another key.[23]

Section 2(1)(f)[24] define an "asymmetric crypto system" as a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature".

iii.Hash Key (Cryptographic Hash Function):

A hash key, often referred to as a cryptographic hash function, is a mathematical process that transforms the information being input into an encrypted sequence of symbols with a defined size. This resulting string is commonly known as a hash value

[21] Schedule V, The Information Technology (Certifying Authorities) Rules, 2000.
[22] Image Source: https://litux.nl/mirror/securitytools/ddu/ch09lev1sec1.html.
[23] S.Suguna et. al.,*A study on symmetric and asymmetric Key Encryption algorithms*, 3(4) INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY, 29, 29 -31(2016).
[24] S.2(1)(f), The Information Technology Act, 2000.

or hash code. Cryptographic hash functions possess key attributes such as determinism (wherein identical inputs consistently yield identical outputs), irreversibility (making it computationally impractical to reconstruct the original data from the hash value), and collision resistance (wherein the likelihood of two distinct inputs generating the same hash value is minimal). Hash functions are often employed in cryptography for a range of applications, such as ensuring the integrity of data, hashing passwords, creating digital signatures, and generating message authentication codes (MACs). They have a vital function in guaranteeing the accuracy and genuineness of digital information by generating a distinct fingerprint or checksum for data, which may be utilised to identify any unauthorised alterations or tampering.

iv. Session Keys:

Session keys are ephemeral cryptographic keys that are created for the purpose of a specific communication session or data exchange. These keys are frequently generated from either symmetric or asymmetric keys and are employed to encrypt data throughout a session. Session keys enhance security by minimising the vulnerability of long-term cryptographic keys and decreasing the likelihood of them being compromised. They are commonly used in secure communication protocols like SSL/TLS to encrypt internet traffic during online sessions.[25]

v. Key Derivation Functions (KDFs):

Key derivation functions are cryptographic algorithms used to derive additional keys from existing keys or secret values. KDFs play a crucial role in generating session keys, keying materials, and cryptographic parameters for various cryptographic protocols and applications. They ensure that derived keys possess sufficient randomness and entropy to resist cryptographic attacks and provide adequate security for cryptographic operations.[26]

In summary, cryptographic keys are essential components of modern cryptography, enabling secure communication, data protection, and authentication in digital

[25] Available at https://www.cs.unibo.it/babaoglu/courses/security/resources/documents/intro-to-crypto.pdf.

[26] Chuah, Chai Wen & Dawson, Ed & Simpson, Leonie. (2013). Key derivation function: The SCKDF scheme, IFIP Advances in Information and Communication Technology. 405. 125-138. 10.1007/978-3-642-39218-4_10.

environments. Whether symmetric or asymmetric, these keys are instrumental in ensuring the confidentiality, integrity, and authenticity of sensitive information exchanged between parties. Proper key management practices, including key generation, distribution, storage, and rotation, are essential for maintaining the security of cryptographic systems and safeguarding against potential vulnerabilities and threats.

II. INTERNATIONAL STANDARDS

International encryption standards are essential in determining the regulations that regulate the usage and application of cryptographic technology worldwide. These standards, set by respected organisations and consortia, offer recommendations, optimal methods, and technical specifications to guarantee interoperability, security, and compatibility in the worldwide encryption ecosystem.

Cryptography plays a crucial role in the worldwide cybersecurity arena by guaranteeing the secrecy, accuracy, and legitimacy of digital data. International standards are essential for governing cryptographic methods, establishing acceptable degrees of encryption, and facilitating compatibility across different countries. This section offers a summary of the global standards that regulate cryptography and explains the acceptable degrees of encryption set by influential regulatory organisations.

Global encryption standards are crucial for establishing the rules that govern the use and implementation of cryptographic technologies on a global scale. Above mentioned organisations and consortia establish these standards to provide suggestions, ideal approaches, and technical specifications that ensure interoperability, security, and compatibility in the global encryption ecosystem.
Cryptography is essential in the global cybersecurity field since it ensures the confidentiality, integrity, and authenticity of digital information. International standards are necessary for regulating cryptographic techniques, determining acceptable levels of encryption, and promoting interoperability across various nations. This section provides a concise overview of the worldwide standards governing cryptography and elucidates the permissible levels of encryption established by important regulatory bodies.

Encryption Levels:

The acceptable thresholds of encryption, as mandated by global standards, differ based on the specific purpose and legal objectives. Encryption techniques are often categorised into three tiers according to their key lengths and computational complexity: symmetric encryption, asymmetric encryption, and hash functions.

In the case of Symmetric encryption techniques, such as AES[27] and DES, employ a single key for both the encryption and decryption processes. The acceptable key lengths for symmetric encryption methods usually vary between 128 bits and 256 bits, as defined by standards such as ISO/IEC 18033-2 and NIST SP 800-38A.[28]On the other hand, in the case of Asymmetric encryption algorithms, including RSA and Elliptic Curve Cryptography (ECC), employ separate keys for encryption and decryption. The permissible key lengths for asymmetric encryption algorithms vary significantly, with RSA key lengths ranging from 1024 bits to 4096 bits and ECC key lengths typically ranging from 160 bits to 521 bits.[29]

Hash functions, such as SHA-256 and SHA-3, are cryptographic algorithms used for data integrity verification and digital signatures. The permissible output lengths for hash functions are defined by standards such as ISO/IEC 10118 and NIST SP 800-107, with commonly used output lengths including 128 bits, 256 bits, and 512 bits.

III. INDIAN STANDARDS OF ENCRYPTION

In India, an executive order authorized the interception of communications under Section 5(2) of the Telegraph Act of 1885 and Section 69B of the Information Technology Act of 2000. (Hereinafter IT Act).

License Restrictions, 1999

In 1999, the Department of Telecommunications (DOT) imposed limitations on the level of encryption strength. As per a revision by the Department of Telecommunications (DOT) to the licencing of Internet Service Providers (ISPs), individuals, organisations, and businesses

[27] NIST, "FIPS PUB 197: Advanced Encryption Standard (AES)." Available at https://csrc.nist.gov/publications/detail/fips/197/final.
[28] *Ibid.*
[29] *Ibid.*

are only allowed to utilise a key length of 40 bits without obtaining prior clearance. Increasing the key size would require the providers to obtain government clearance.

Information Technology (Certifying Authorities) Rules 2000

The norms and regulations of the certifying authority in information technology pertain to encryption. Rule 6 of IT rules 2000 provides standards for certifying authorities. The IT Rules 2000 provide that digital communication devices can be equipped with suitable encryptors or encryption software for conveying secret content.[30] Likewise, it is imperative to encrypt any really sensitive information and data in order avoid illicit accessibility. The government have the authority to determine the level of encryption necessary for safeguarding electronic records that require privacy.[31]

Information Technology Act, 2000

In order to bring it into step with constantly changing technology, the Information Technology Act 2000 was modified in 2008. A major development was the introduction of Section 84A[32] that enabled the government to regulate encryption techniques and modes to encourage E-government and e-commerce. Section 69[33], which enables the central and state governments to intercept and decode information essential to defend national security, preserve public order or investigate crimes, has also led to another modification. The clause also requires users and service providers to support the access by law enforcement officials and government organizations.

Information Technology (Procedure and Safeguard for interception, Monitoring and Decryption Rules), 2009 [34]

The government developed the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules 2009 shortly after these changes were passed. The parameters of decryption and the necessary procedure were clarified by these regulations. Decryption assistance, for example, was described as giving

[30] Schedule I Rule 5.2(6).

[31]t Rule 5.3(1).

[32] Supra Note 8 at S.84A

[33] Ibid at S.69

[34] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption Rules) 2009 (hereafter referred to as the Decryption Rules).

information access to the degree feasible and only when the intermediary had authority over the decryption keys.[35]

Rule 3 of decryption rule says about the direction for interception or monitoring or decryption of any information.[36]In most cases, obtaining authorization from the appropriate authority is necessary to access, track, or decode any data stored in a computer system. However, in rare cases, a government representative no lower than the Joint Secretary of the Republic of India who has been officially authorised by the appropriate authorities can issue such an order. Within seven days of the order's issuance, it must be forwarded to the review committee.[37] Such order shall be limited to the information is encrypted and intermediaries have control over the decryption key.[38]

BlackBerry Case, 2007 – 2012

The initial significant event involving the conflict between encryption and national security arose when the Indian government mandated Research in Motion's (RIM) BlackBerry to provide law enforcement with the ability to access its encrypted data. RIM, as a device maker, was exempt from the encryption regulations that apply to telecommunications firms under the licence agreements. On December 31, 2007, the Department of Telecommunications (DOT) requested the business to cease its services in India after recognising their inability to oversee the information transmitted through BlackBerry handsets. The Indian government issued a warning to telecom providers, stating that they will be instructed to terminate BlackBerry services unless the business enabled the legal interception of encrypted conversations in India. The demands increased significantly after it was discovered that the terrorists responsible for the 2008 terror attacks in Mumbai had utilised BlackBerry handsets to communicate with their handlers in Pakistan.

National Encryption Policy, 2015 (Drafted):

In September 2015, the union government introduced the draft National Encryption Policy, marking an important occasion. The strategy sought to develop precise procedures and mathematical procedures for encoding information, exchanging secret codes, and verifying

[35]*Id.* at Rule 2(g) (i).
[36]*Ibid.*
[37]*Ibid* at Rule 7.
[38]*Ibid* at Rule 13(3).

the authenticity of digital documents for government institutions, enterprises, and private users. Unlike prior regulations, such as those outlined in the Unified Services licence, this policy does not set any specific restrictions on the strength or kind of encryption used. However, it permitted unrestricted use of encryption as long as users complied with requests from law enforcement authorities.

In order to guarantee this collaboration, the policy enforced rigorous responsibilities on both corporations and individuals. The policy prescribed:

- Encryption product vendors, except those offering widely-used services such as SSL and Transport Layer Security, must register their goods with the government and provide functional copies of the software and hardware used for encryption.[39]
- Service providers must engage in an agreement with the Indian government if they utilise encryption.[40]Although the specific details of the agreement were not made clear, it was a need for conducting business in India.
- Businesses are required to provide the encrypted text, plaintext, hardware, and software used for encryption when they get a request from law authorities.[41]
- Users are required to save the unencrypted version of their encrypted data on their devices for a period of ninety days, in case law enforcement authorities request access to this information.[42]

Other Laws and Regulations

❖Security and Exchange Board if India (SEBI)

The Report on Internet Trading through the Securities Exchange Board India Committee on Internet-based Trading & Services, 2000, suggests using a 64/128-bit encryption standard to protect all operations, including online trading. It is highly recommended to freely use 128-bit encryption. However, the clause specifies that the encryption policy of the Department of Telecommunications would be adhered to.

❖Reserve Bank of India (RBI)

[39] Clause V (1), Draft National Encryption Policy 2015.
[40] I*bid*, Clause IV (6).
[41]*Ibid,* Clause IV (4).
[42]*Ibid*, Clause IV (5) and (7).

The Reserve Bank of India, in its 2001 Report on Internet Banking, required the implementation of a minimum-security level for server authentication using the Secure Socket Layer, as well as the usage of client-side certificates. The text states that 128-bit SSL encryption is used to secure communication between browsers and servers. This encryption is applied to sensitive data, such as passwords, while it is being sent within the company.

❖ Development

Recently Social media Guidelines (2021)[43], which make provisions that:

> "*A significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed under Section 69 of the Act by the Competent Authority asper the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information)Rules, 2009, which shall be supported with a copy of such information in electronic form.*"

Also required by the rules is that middlemen designate a nodal officer who would work around the clock to ensure that law enforcement is above mentioned instructions.

IV. CONCLUSION

Given the importance of cybersecurity, privacy, and national security, India need a robust encryption/decryption framework to effectively satisfy the concerns of the information technology sector and law enforcement authorities. The private sectors must continuously adapt and evolve to stay abreast of technological advancements. Their capacity to counter cybersecurity risks and safeguard their technical infrastructure from such threats mostly relies on the existence of a well-defined national framework or regulatory environment. Any rule regarding encryption should not force private parties to choose between using weaker encryption or bearing the cost of providing prior notification and decryption key escrow for better encryption. This rule, particularly for an Internet Service Provider, might be too

[43] "Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021," Ministry of Electronics and Information Technology, Available at http://egazette.nic.in/WriteReadData/2021/225464.pdf.

burdensome since it may discourage private companies from using strong encryption. This, in turn, could increase India's susceptibility to cyber-attacks. It should be emphasised that the need of notification and deposit is often the standard practice in other jurisdictions. Hence, it is imperative that any legislation pertaining to encryption, as established by the Government, exhibit flexibility and adaptability in order to keep pace with the ever-evolving advancements in encryption technology. Additionally, it is imperative for the Government to guarantee that encrypted conversations or data do not traverse any intermediary or government representative who may exploit such encrypted communications.