Balancing National Security and Personal Privacy: Legal Implications of Encryption Backdoors in Global Cybersecurity Policy

1. Anjali Sharma*: Department of International Trade Law, University of Delhi, Delhi, India

*Correspondence: e-mail: Anjalisharm15@gmail.com

Abstract

The debate surrounding encryption backdoors has become a critical issue in the context of national security and personal privacy. As digital technologies advance, encryption has emerged as a cornerstone for protecting sensitive data, ensuring secure communications, and safeguarding individual privacy. However, governments, particularly those focused on combating terrorism, cybercrime, and other security threats, have increasingly advocated for the introduction of encryption backdoors to allow law enforcement agencies to access encrypted data. This article explores the legal, technical, and ethical implications of encryption backdoors, focusing on the balance between securing personal privacy and addressing national security concerns. It delves into the role of encryption in protecting personal privacy, the potential risks associated with backdoors, and the challenges they pose to global cybersecurity policy. The article also examines divergent national approaches to encryption, highlighting the contrasting positions taken by countries such as the United States, the United Kingdom, China, and members of the European Union. Furthermore, it considers the technical difficulties in implementing backdoors, including the vulnerability they introduce to data security, as well as the policy and governance challenges in creating international frameworks that accommodate both privacy rights and security needs. Finally, the article discusses the role of public perception and trust in shaping government decisions related to encryption and privacy, emphasizing the need for continued dialogue between policymakers, cybersecurity experts, and the technology industry to find balanced solutions. This review provides a comprehensive analysis of the ongoing tension between national security and personal privacy, offering insights into the future direction of global cybersecurity policy and legal frameworks.

Keywords: Encryption, Backdoors, National Security, Personal Privacy, Cybersecurity, Legal Implications

Received: 10 August 2022
Revised: 13 September 2022
Accepted: 26 September 2022
Published: 01 October 2022

Citation: Sharma, A. (2022). Balancing National Security and Personal Privacy: Legal Implications of Encryption Backdoors in Global Cybersecurity Policy. *Legal Studies in Digital Age*, 1(1), 53-67.

1. Introduction

In the digital age, the tension between national security and personal privacy has become one of the most challenging and debated issues in cybersecurity policy. As technology advances, especially in the realm of communication and data protection, encryption has become a cornerstone in safeguarding personal privacy and ensuring secure communication. At the same time, governments across the globe argue that the widespread use of strong encryption technologies poses significant challenges to

national security, law enforcement, and counterterrorism efforts. Encryption, while serving as a powerful tool for privacy protection, can also hinder investigations into criminal activity, leaving governments and security agencies seeking ways to bypass these security measures without violating citizens' fundamental rights. The debate intensifies when it comes to the introduction of encryption backdoors—deliberate weaknesses embedded in encryption systems to allow government agencies or other entities authorized by law to access encrypted data. Proponents of encryption backdoors argue that they are necessary to combat cybercrime and terrorism, while critics assert that they undermine the very security and privacy that encryption is meant to protect.

The primary concern surrounding encryption backdoors is the delicate balance between national security needs and the protection of personal privacy. National security demands often call for access to encrypted communications to track terrorist activities, prevent cyberattacks, and investigate organized crime. Governments around the world, particularly in jurisdictions where threats of terrorism and state-sponsored cyberattacks are prominent, view encryption backdoors as essential tools to preserve public safety and the integrity of national borders. However, the push for encryption backdoors directly challenges the core principle of individual privacy. Encryption systems are designed to ensure that data transmitted between users is unreadable to unauthorized parties. A backdoor inserted into these systems would effectively create an opening for governments or hackers to access private information, potentially exposing sensitive data to malicious actors (Taramonli et al., 2012; Watzlaf et al., 2011). Furthermore, once backdoors are introduced, the question arises: who controls these backdoors, and how can their use be regulated to prevent abuse? The implementation of such systems could open the floodgates to widespread surveillance, data breaches, and exploitation of personal information, thereby eroding trust in digital communication platforms.

The growing reliance on encrypted platforms, such as messaging apps and cloud storage services, only amplifies the significance of this debate. Messaging applications, in particular, are widely used for both personal and professional communication, often including confidential or sensitive information. The advent of end-to-end encryption (E2EE), where only the communicating parties can decrypt the messages, has raised alarms in governments, especially in relation to the inability of law enforcement to access communications in investigations. The argument is made that in cases of national security threats, the inability to access encrypted data may prevent the prevention of terrorist attacks or organized criminal activity. On the other hand, the very technologies that governments seek to control—end-to-end encryption and secure messaging platforms—are integral to maintaining personal freedoms and privacy. Without them, the risk of unchecked surveillance and loss of privacy could outweigh the perceived benefits to national security (Liu & Ren, 2013; Popa et al., 2013). The challenge lies in finding a solution that addresses both security concerns and privacy rights without tipping the scale too far in either direction.

The purpose of this review is to examine the legal implications of encryption backdoors, focusing on how these mechanisms intersect with global cybersecurity policy. The review aims to critically assess the impact of encryption backdoors on both national security and personal privacy, exploring the intricate legal landscape that governs the use of such technologies. It will delve into various legal frameworks that aim to balance these competing interests, drawing on real-world examples and case studies to highlight the complexities and consequences of introducing encryption backdoors. By analyzing both the legal and technological aspects of this issue, the review will seek to uncover the implications of encryption backdoors on individuals' fundamental rights and freedoms, as well as the broader cybersecurity ecosystem. As encryption backdoors become a focal point of policy debates in the realms of digital governance, this review will also explore how international norms, agreements, and regulations can contribute to a more harmonized approach to encryption and privacy laws. Additionally, the review will consider the role of encryption in global cybersecurity and its significance in maintaining the security of digital infrastructure and personal data in a rapidly evolving technological landscape. Ultimately, the goal is to provide a comprehensive understanding of the legal, ethical, and technical dimensions of encryption backdoors, informing both policymakers and the public about the stakes involved in this high-stakes issue.

As such, the review will also examine how different jurisdictions have responded to the challenge of balancing encryption with national security concerns. In some countries, governments have pushed for legislation that would mandate the creation of backdoors in encryption software to facilitate lawful interception. In others, there is strong resistance to such measures, based on the belief that any compromise in encryption security would have far-reaching negative consequences for individuals' privacy and the integrity of digital communications.

2. Understanding Encryption and Encryption Backdoors

Encryption is a fundamental technology in modern cybersecurity, designed to protect sensitive information from unauthorized access by transforming data into an unreadable format using complex algorithms. The primary function of encryption is to secure the transmission and storage of data, ensuring that only authorized parties, typically through the use of decryption keys, can access and interpret the original information. This process is essential for maintaining confidentiality, integrity, and authenticity in digital communications, making it a critical component in securing personal data across various platforms, such as email, messaging, and financial transactions. Without encryption, data transferred over networks, including the internet, would be vulnerable to interception and exploitation, compromising both individual privacy and institutional security. In this context, encryption is widely used in numerous applications ranging from securing personal devices and online banking transactions to safeguarding sensitive communications in sectors such as healthcare, finance, and government (Abu-Salma, Sasse, et al., 2017; Kerschbaum & Härterich, 2017; Samiullah et al., 2022; Shi et al., 2022).

At its core, encryption employs mathematical algorithms to convert plaintext data into ciphertext. This conversion involves a key, which is a piece of data used to both encrypt and decrypt the information. The security of encrypted data relies on the complexity of these algorithms and the length of the encryption key, with longer keys offering a higher level of security. There are two main types of encryption: symmetric encryption, where the same key is used for both encryption and decryption, and asymmetric encryption, which involves a public key for encryption and a private key for decryption. Public key encryption is commonly used in systems like Secure Sockets Layer (SSL) for internet security, while symmetric encryption is often employed for encrypting data stored on devices or in cloud storage. As encryption technology has evolved, so too have the sophistication and robustness of these algorithms, with continuous efforts to improve encryption standards in response to emerging threats (Distler et al., 2020; Hidayat & Mahardiko, 2020).

Despite its widespread use, encryption has become a contentious issue, particularly in the context of national security. Governments, law enforcement, and intelligence agencies argue that while encryption plays a vital role in protecting individual privacy and security, it also complicates efforts to combat crime, terrorism, and cyberattacks. One of the most debated aspects of this issue is the concept of encryption backdoors—deliberate vulnerabilities inserted into encryption systems to provide authorized entities with a means of accessing encrypted data without requiring the decryption key. Encryption backdoors are typically presented as a solution to facilitate investigations into criminal activities, enabling authorities to bypass encryption and access potentially vital evidence that would otherwise be hidden. However, the introduction of backdoors into encryption systems raises serious concerns about security and privacy, as it creates a potential entry point for malicious actors, including hackers and rogue governments, to exploit (Yang et al., 2019).

An encryption backdoor is essentially a hidden access point that bypasses the encryption process, allowing unauthorized users to decrypt encrypted data without the need for a valid decryption key. While backdoors may be authorized for use by government agencies or law enforcement under certain circumstances, they inherently weaken the overall security of the encryption system. Once a backdoor is embedded into a system, it introduces a potential vulnerability that could be exploited by cybercriminals or foreign adversaries to gain unauthorized access to sensitive data. The security of encrypted data hinges on the assumption that only the intended recipients possess the decryption key, but backdoors compromise this fundamental principle by opening up a way for others, including those who might misuse the access, to decode the data. In addition to the risk of unauthorized access, backdoors also create the possibility of systemic vulnerabilities. Even if the backdoor is intended to be used exclusively by authorized entities, there is always the risk that it could be discovered or exploited by malicious actors, thereby undermining the very security that encryption was meant to provide (Hasanova et al., 2019).

The idea of introducing encryption backdoors is not new, and there have been several notable instances where government agencies or private companies have sought to incorporate such features into encryption systems. One of the most infamous cases occurred in the mid-1990s with the introduction of the Clipper Chip. The Clipper Chip was a government initiative that aimed to embed a backdoor into secure telecommunications systems, allowing law enforcement agencies to monitor encrypted communications without the knowledge of the parties involved. The Clipper Chip was designed to provide secure voice communications by encrypting phone calls using a government-approved algorithm, with a built-in backdoor that could be accessed by authorities with the appropriate decryption key. The initiative faced widespread criticism from privacy advocates, who argued that the backdoor posed a severe threat to individual privacy and civil liberties. The Clipper Chip ultimately failed

due to both technical flaws and public resistance, highlighting the challenges of balancing national security interests with the protection of personal freedoms (Nojeim & Maheshwari, 2021).

Another well-known example of the encryption backdoor debate emerged in 2016 with the FBI-Apple encryption controversy. In this case, the FBI requested that Apple assist in unlocking an iPhone that belonged to one of the perpetrators of the San Bernardino terrorist attack. The FBI sought to compel Apple to create a backdoor into the iPhone's encryption, which would allow the agency to bypass the device's security features and access the data stored on it. Apple refused to comply, citing concerns about the security implications of creating such a backdoor and the potential for setting a dangerous precedent. The case ignited a fierce debate about the role of technology companies in enabling government access to encrypted data. While the FBI argued that unlocking the phone was crucial to the investigation, Apple and other tech companies contended that creating a backdoor would undermine the security of all iPhones, leaving users vulnerable to hacking and unauthorized surveillance. This case exemplified the difficult trade-offs between national security and personal privacy and highlighted the potential consequences of introducing encryption backdoors (Samiullah et al., 2022).

These examples demonstrate the complexities and risks associated with encryption backdoors. On one hand, proponents of backdoors argue that they are necessary tools for ensuring national security and law enforcement capabilities in an increasingly digital world. They point out that strong encryption can be a barrier to criminal investigations, preventing authorities from gaining access to crucial evidence. On the other hand, critics warn that backdoors compromise the very security that encryption is meant to provide, exposing individuals and organizations to a range of risks, from cyberattacks to unauthorized surveillance. The debate is further complicated by the fact that encryption backdoors, if introduced, would create a universal vulnerability that could be exploited by malicious actors, not just governments and law enforcement. In this sense, encryption backdoors represent a double-edged sword, offering potential benefits for national security while simultaneously creating new and significant risks to cybersecurity and personal privacy (Chandravathi, 2018; Endeley, 2018).

In conclusion, encryption plays a pivotal role in modern cybersecurity, protecting sensitive information from unauthorized access and ensuring the confidentiality of communications. However, the introduction of encryption backdoors presents a complex challenge to the balance between national security and personal privacy. While encryption backdoors are argued to be necessary tools for law enforcement and national security purposes, they also introduce significant risks to data security, privacy, and trust in digital systems. The examples of the Clipper Chip and the FBI-Apple case illustrate the ongoing struggle to find a solution that adequately addresses both security concerns and individual rights, leaving open the question of whether encryption backdoors can be effectively and safely implemented without compromising the core principles of cybersecurity and privacy.

3. National Security Concerns and the Need for Encryption Backdoors

Cybersecurity has emerged as one of the most significant challenges facing governments and international organizations today. The rise of digital technologies has transformed the global landscape, offering unprecedented convenience and efficiency but also giving rise to a host of new threats. Among these threats, terrorism, cyberattacks, and state-sponsored hacking have become the primary concerns driving governments to seek ways to circumvent encryption technologies. These security challenges are not only increasingly complex but also highly disruptive, as cybercriminals, terrorist organizations, and hostile nation-states leverage sophisticated digital tools to achieve their goals. For instance, the use of encrypted communication platforms has become a standard practice for terrorist organizations, allowing them to operate with a high degree of secrecy, evade surveillance, and plan attacks with minimal detection. Additionally, state-sponsored hacking groups have utilized encryption to exfiltrate sensitive data, undermine democratic processes, and engage in cyber-espionage without detection. The nature of these threats has prompted governments worldwide to reconsider how encryption can be both a tool for safeguarding citizens and a potential barrier to effective law enforcement and national security measures (Abu-Salma, Krol, et al., 2017; Kumar et al., 2014; Kumar & Chahal, 2014; Li et al., 2015).

Encryption plays a central role in protecting personal privacy and securing communications, making it an indispensable tool in today's digital age. Individuals rely on encryption to ensure the confidentiality of their communications and financial transactions, and businesses depend on it to protect sensitive data and maintain customer trust. However, from a national security perspective, the widespread use of strong encryption poses a significant challenge for law enforcement agencies tasked

with investigating and preventing cybercrime, terrorism, and other security threats. In particular, encryption enables criminals and terrorists to operate under the radar, making it difficult for authorities to monitor their activities and gather critical intelligence. This has led governments to argue that law enforcement must have access to encrypted data in specific cases, even if that requires undermining the very security that encryption provides (Hidayat & Mahardiko, 2020; Liu & Ren, 2013).

The role of encryption in national security is deeply paradoxical. On one hand, encryption is a vital tool for protecting citizens' privacy and securing national infrastructure, particularly in the face of growing cyber threats. Without strong encryption protocols, sensitive data would be vulnerable to theft, and individuals and organizations alike would be exposed to the risk of cyberattacks. On the other hand, encryption also complicates national security efforts by making it more difficult for governments to monitor and investigate potential threats. Terrorist groups, for example, have increasingly turned to encrypted messaging apps and other secure communication platforms to evade surveillance and coordinate attacks. These platforms, often using end-to-end encryption, ensure that only the sender and recipient can read the content of the communication, leaving law enforcement agencies with little to no means of intercepting or decrypting the messages. From the perspective of security agencies, this creates a significant problem, as encrypted communication serves as a shield that prevents them from gathering intelligence in real-time, ultimately hindering their ability to prevent terrorist activities or disrupt criminal networks. Thus, the challenge lies in balancing the benefits of encryption for privacy and security with the need for lawful access to encrypted communications to protect national security (Samiullah et al., 2022; Spinello, 2020).

Governments have responded to this challenge by seeking to develop and implement measures that would allow them to access encrypted data without compromising the integrity of encryption systems. One of the most contentious proposals has been the introduction of encryption backdoors. These backdoors are essentially intentional vulnerabilities or weaknesses built into encryption systems that allow third parties, such as government agencies, to bypass encryption and gain access to encrypted data. Proponents of encryption backdoors argue that they are essential for enabling law enforcement agencies to gather critical intelligence and prevent national security threats. However, critics argue that encryption backdoors inherently weaken the security of encryption systems, creating openings for malicious actors, including hackers and cybercriminals, to exploit these vulnerabilities for their own gain. Once backdoors are introduced into a system, it becomes difficult to ensure that they will only be used for legitimate purposes. In this sense, encryption backdoors present a fundamental dilemma: how to balance the need for national security with the imperative to safeguard individual privacy and the integrity of encryption systems (Li et al., 2022).

Several case studies illustrate the challenges that encryption presents to national security and the complex decisions governments must make in the face of these issues. One notable example is the debate between law enforcement agencies and technology companies over access to encrypted data in the wake of the 2015 San Bernardino terrorist attack in the United States. In this case, the FBI sought to compel Apple to assist in unlocking an iPhone that belonged to one of the attackers, arguing that the phone contained vital information that could help prevent future attacks. Apple refused, citing the importance of encryption in protecting user privacy and the potential risks of creating a backdoor into the phone. The case sparked a heated public debate over the role of encryption in national security and whether governments should have the ability to compel companies to create vulnerabilities in their systems. While the FBI eventually found a third-party solution to unlock the phone, the case highlighted the growing tension between national security concerns and the protection of individual rights, particularly in an age where data privacy is a fundamental aspect of personal freedom (Li et al., 2022; Samiullah et al., 2022).

Another relevant case is the "Clipper Chip" controversy in the 1990s. In an attempt to allow government agencies to access encrypted communications, the U.S. government proposed the Clipper Chip, a hardware-based encryption system that would have embedded a backdoor known as the "Key Escrow" system. This system would have allowed the government to hold the decryption keys to all encrypted communications, ostensibly for use in national security and law enforcement investigations. However, the Clipper Chip was met with widespread opposition from privacy advocates, security experts, and technology companies, who argued that embedding a backdoor into encryption systems would undermine the security of all communications and open the door for abuse. Critics also pointed out that once the backdoor was created, there was no way to guarantee that it would not be exploited by malicious actors. The controversy over the Clipper Chip eventually led to its abandonment, but it set the stage for ongoing debates about encryption and backdoors that continue to this day (Hasanova et al., 2019; Samir & Raissouni, 2019; Yang et al., 2019).

Other incidents involving encryption have further demonstrated the challenges faced by governments in addressing national security concerns. For example, state-sponsored hacking groups, such as those involved in cyber-espionage or political interference, often rely on encryption technologies to protect their communications and data. These groups, which may operate under the auspices of a national government, use encryption to shield their activities from detection, making it difficult for law enforcement or intelligence agencies to track their movements or prevent attacks. In some cases, these actors have been able to penetrate sensitive governmental or corporate systems without leaving a trace, thanks to the strength of the encryption technologies they employ. This has prompted governments to explore ways to weaken or bypass encryption, often invoking the need to protect national interests or prevent cyberattacks from foreign adversaries (Chandravathi, 2018; Rodriguez & Centonze, 2017; Usman et al., 2017).

In summary, the need for encryption backdoors is driven by a complex array of national security concerns, from the fight against terrorism to the defense against cyberattacks and state-sponsored hacking. While encryption plays a crucial role in safeguarding individuals' privacy and securing national infrastructure, it also presents significant challenges for governments tasked with preventing and responding to security threats. The debate over encryption backdoors highlights the difficulty of striking a balance between protecting privacy and ensuring national security. As the digital landscape continues to evolve, the issue of encryption and its role in national security will remain a key area of contention, requiring careful consideration of the trade-offs between security and civil liberties.

4. Personal Privacy and the Right to Encryption

Privacy has long been recognized as a fundamental human right, essential to the protection of individual freedoms and the maintenance of a democratic society. The right to privacy is enshrined in numerous international legal instruments, including the Universal Declaration of Human Rights, which affirms that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.” This principle is further reinforced in regional frameworks such as the European Convention on Human Rights, which upholds the right to respect for private and family life. Additionally, the right to privacy has been incorporated into national legal systems, with constitutional protections in many countries safeguarding citizens from unwarranted intrusions. Privacy laws, including the General Data Protection Regulation (GDPR) in the European Union, reflect an evolving understanding of privacy in the digital age, where individuals’ personal data has become a valuable commodity. The GDPR, in particular, emphasizes the right of individuals to control their personal information, placing stringent requirements on organizations to protect data and provide transparency about its use. As such, the legal foundations of privacy are not only about safeguarding the physical space of individuals but also ensuring that their personal information remains protected from unauthorized access and exploitation in the digital realm (Distler et al., 2020; Hidayat & Mahardiko, 2020; Samir & Raissouni, 2019; Yang et al., 2019).

In this context, encryption has emerged as one of the most effective tools for protecting personal privacy and securing sensitive data. Encryption technologies function by transforming readable data into an unreadable format using complex algorithms, ensuring that only authorized parties with the correct decryption keys can access the original information. This process is fundamental to securing personal communications, protecting financial transactions, and maintaining the confidentiality of sensitive information stored on personal devices or in the cloud. As digital communication becomes more ubiquitous, the need for encryption has grown exponentially, as individuals rely on it to safeguard everything from personal messages to banking details and medical records. Without encryption, personal data would be vulnerable to a wide range of threats, including cyberattacks, identity theft, and unauthorized surveillance. Encryption not only enhances security but also ensures that individuals can exercise their right to privacy in an increasingly interconnected world (Chandravathi, 2018; Chen et al., 2019; Endeley, 2018).

However, the introduction of encryption backdoors represents a direct threat to personal privacy, as these mechanisms can compromise the very security that encryption is meant to provide. Encryption backdoors are designed to create intentional vulnerabilities in encryption systems, allowing authorized parties—typically law enforcement agencies or intelligence services—to bypass encryption and access encrypted data. While proponents of encryption backdoors argue that they are necessary for national security and law enforcement, critics highlight the significant risks these vulnerabilities pose to personal

privacy. The insertion of a backdoor into an encryption system creates an opening for unauthorized actors to exploit, including cybercriminals and hackers. Once a backdoor is introduced, it can be exploited in ways that were never intended, leading to data breaches, identity theft, and the exposure of sensitive information. The potential for backdoors to be misused or accessed by malicious actors undermines the core principle of encryption as a safeguard for personal privacy and data security. Moreover, backdoors could create a "weakest link" in an otherwise secure system, as the very existence of the backdoor introduces an element of risk that could affect millions of individuals (Kumar et al., 2017; Yasser et al., 2020).

The impact of encryption backdoors on privacy is not merely theoretical. There have been several instances where the implementation or compromise of encryption systems has led to significant violations of privacy. For example, in cases where government agencies have attempted to bypass encryption, individuals' private communications have been exposed, resulting in breaches of trust and safety. One of the most notable cases in recent years was the FBI-Apple dispute over unlocking an iPhone used by a terrorist in San Bernardino. The FBI demanded that Apple create a backdoor to bypass the phone's encryption, arguing that this would help them investigate potential terrorist connections. However, Apple refused, citing the potential harm that creating such a backdoor could cause to the privacy of all its users. The company argued that creating a universal backdoor for one case would set a dangerous precedent, opening the door for further government demands and potentially compromising the privacy of millions of individuals. The case highlighted the ethical and legal dilemmas surrounding encryption backdoors and the implications they have for personal privacy. If the backdoor had been created, it could have exposed not only the specific individual's information but also the broader user base to potential surveillance or exploitation. This case underscores the fundamental tension between national security interests and the protection of personal privacy .

Another example of the dangers posed by compromised encryption is the history of the "Clipper Chip," a government-backed initiative in the early 1990s aimed at implementing mandatory encryption standards for telecommunications. The chip contained a built-in backdoor, which allowed the government to monitor encrypted communications if needed. While proponents argued that it was necessary for national security, the public and private sectors, including major technology companies, strongly opposed it. They argued that such a system would undermine trust in encrypted communications and expose users to privacy risks. Ultimately, the Clipper Chip was abandoned, but it served as an early example of the risks posed by backdoor encryption systems. The failure of the Clipper Chip reinforced the concerns that encryption backdoors could lead to the erosion of privacy and the potential for widespread surveillance (Hasanova et al., 2019; Samir & Raissouni, 2019; Yang et al., 2019).

In more recent years, there have been several incidents where backdoors or vulnerabilities in encryption systems have been exploited by malicious actors. For instance, the revelations about the vulnerability known as "Heartbleed," which affected the widely used OpenSSL cryptographic software, exposed the sensitive data of millions of users. While Heartbleed was not an intentional backdoor, its existence demonstrated how weaknesses in encryption systems could be exploited to gain unauthorized access to private data. In cases where backdoors are intentionally introduced, the consequences could be even more severe. Hackers could exploit these vulnerabilities to gain access to individuals' personal information, financial records, or communications, leading to identity theft, financial loss, and reputational damage. As such, the introduction of backdoors into encryption systems represents not only a threat to national security but also to the very fabric of privacy that underpins democratic societies (Li et al., 2022; Samiullah et al., 2022; Shi et al., 2022; Yazdeen et al., 2021).

The risk of introducing backdoors is not just hypothetical—it has tangible, real-world consequences for individuals' privacy and security. For example, in countries where surveillance laws are less robust and government overreach is more common, encryption backdoors could be used to monitor citizens without proper legal safeguards or oversight. In such contexts, encryption backdoors could facilitate widespread violations of privacy, disproportionately affecting marginalized communities or political dissidents. Additionally, in nations with less stringent data protection laws, the exploitation of encryption backdoors could lead to mass surveillance, unauthorized data collection, and other forms of privacy violations. These risks highlight the potential dangers of allowing backdoors into encryption systems, which can undermine not only the security of digital communications but also the broader principles of privacy and freedom (Nojeim & Maheshwari, 2021; Yasser et al., 2020).

In conclusion, while encryption is a vital tool for protecting personal privacy and data security in the digital age, the introduction of encryption backdoors presents significant risks. Backdoors create vulnerabilities in encryption systems, exposing individuals' sensitive data to unauthorized access and exploitation. The potential for these backdoors to be misused

or compromised by malicious actors represents a direct threat to personal privacy and individual freedom. As the global debate surrounding encryption and national security continues, it is essential to carefully consider the long-term implications of compromising encryption in the name of security. Ultimately, any attempt to weaken encryption through the introduction of backdoors must be weighed against the potential harm to individual privacy and the broader societal impact. The tension between privacy and security is a complex issue that requires a careful, balanced approach to ensure the protection of both citizens' rights and national security interests.

5. Legal and Ethical Implications of Encryption Backdoors

The legal and ethical implications of encryption backdoors are complex and multifaceted, intertwining with various international laws, human rights frameworks, and national security concerns. In recent years, governments worldwide have faced intense pressure to devise policies that address the growing tension between the necessity of encryption for data protection and the desire for access to encrypted communications for security purposes. The introduction of encryption backdoors—deliberate vulnerabilities or access points that would allow governments or authorized agencies to decrypt communications—raises critical questions about the balance between personal privacy and national security. These challenges are compounded by divergent legal frameworks that operate at the international, regional, and national levels, each with its own set of priorities and objectives.

International legal frameworks play a significant role in shaping the debate around encryption and backdoors. One of the most influential legal instruments in the realm of privacy is the European Union's General Data Protection Regulation (GDPR), which has become a benchmark for privacy laws worldwide. The GDPR mandates that individuals have the right to control their personal data and that data controllers (such as companies and organizations) must ensure the security and integrity of the data they collect. Encryption is recognized as one of the most effective means to protect personal data, and under the GDPR, the use of encryption is encouraged as a tool for safeguarding data subject to processing. However, the regulation also provides exceptions for law enforcement access, particularly in cases of national security or criminal investigations. This duality reflects the broader tension between protecting individual privacy and addressing national security needs. By mandating the protection of personal data while also allowing exceptions for lawful interception, the GDPR exemplifies the legal balancing act that many countries face when considering encryption backdoors (Nanda et al., 2020).

Similarly, the United States has enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which directly intersects with the encryption backdoor debate. The CLOUD Act was passed in 2018 as part of the US's efforts to facilitate cross-border data access for law enforcement. Under this law, US law enforcement agencies are granted the authority to compel US-based technology companies to provide access to data stored overseas, even if that data is encrypted. The act also includes provisions for international agreements that would allow foreign governments to access data stored in the US, creating a legal framework for accessing encrypted information across borders. Critics of the CLOUD Act argue that it undermines privacy protections and could be used to justify government access to encrypted data without sufficient oversight or safeguards. The conflict between privacy and law enforcement access is central to the debate surrounding the act, as the law enables greater governmental access to encrypted communications but raises concerns about overreach and the erosion of privacy rights (Chandravathi, 2018; Endeley, 2018; Nanda et al., 2020).

In addition to these specific legal frameworks, the ethical dilemmas surrounding encryption backdoors have garnered significant attention. Governments face difficult choices when balancing the need for national security with the right to privacy. On the one hand, encryption is a fundamental tool for protecting individuals from data breaches, cyberattacks, and unauthorized surveillance. On the other hand, governments argue that access to encrypted communications is essential for preventing terrorism, cybercrime, and other national security threats. The ethical challenge lies in determining whether it is justifiable to compromise individual privacy in the name of security. Proponents of encryption backdoors argue that in certain cases, such as terrorism or organized crime investigations, the need for security outweighs privacy concerns. They suggest that a legal framework could be established to regulate the use of backdoors, ensuring that access is granted only in specific circumstances and under strict judicial oversight (Abu-Salma, Krol, et al., 2017; Abu-Salma, Sasse, et al., 2017; Kerschbaum & Härterich, 2017).

Opponents of encryption backdoors, however, highlight the risks of creating such vulnerabilities. They argue that backdoors inevitably create security flaws that could be exploited by malicious actors, including hackers, foreign governments, or rogue employees. Even if backdoors are initially implemented with the best of intentions and under controlled circumstances, the potential for abuse or unintended consequences is high. Furthermore, backdoors could undermine the trust that individuals and businesses place in encrypted communications, damaging the integrity of cybersecurity systems as a whole. The ethical dilemma, therefore, revolves around the question of whether the risks to individual privacy and the potential for misuse of backdoor access can ever be justified by the perceived security benefits (Şahin et al., 2020; Spinello, 2020).

Several legal precedents and court cases have shaped the discourse on encryption and backdoors, most notably the Apple-FBI case, which became a landmark in the debate over encryption and privacy. In 2016, the FBI requested that Apple assist in unlocking an iPhone used by a suspect in a terrorist attack. Apple refused, citing the importance of protecting user privacy and the potential for setting a dangerous precedent by creating a backdoor into its devices. The case brought to the forefront the clash between law enforcement's desire to access encrypted data for national security purposes and the tech company's responsibility to protect user privacy. The court case raised significant questions about whether tech companies should be compelled to cooperate with government agencies in providing access to encrypted data, even if doing so could weaken the security of their products. In the end, the FBI was able to gain access to the phone without Apple's help, but the case sparked a broader debate about encryption, security, and the role of private companies in assisting law enforcement. The Apple-FBI case remains a touchstone in discussions about the legal and ethical implications of encryption backdoors, illustrating the profound consequences of requiring companies to weaken their security systems (Nojeim & Maheshwari, 2021).

In another important case, the US government's attempt to force Microsoft to hand over data stored on servers in Ireland raised questions about jurisdictional authority and the global reach of encryption laws. In this case, Microsoft argued that forcing the company to provide access to data stored in another country violated international law and the sovereignty of foreign governments. The legal battle ultimately led to the CLOUD Act, which sought to address the challenges of cross-border data access. This case highlighted the complexities of global data protection and the difficulties in balancing the need for national security with respect for international privacy laws (Li et al., 2022).

Court cases involving encryption also frequently touch on the broader issues of surveillance and the role of law enforcement in the digital age. The debate over encryption backdoors is not only about specific cases but also about the long-term implications for privacy rights and government surveillance powers. Legal challenges have consistently emphasized the importance of due process and the need for robust safeguards to prevent abuse of power. The concept of "constitutional backdoors," which would grant law enforcement agencies a way to bypass encryption for investigative purposes, has been the subject of significant legal and ethical scrutiny. While some argue that these backdoors could be used responsibly under strict legal frameworks, others contend that the mere existence of such vulnerabilities could lead to widespread abuse and undermine public trust in encryption technologies (Li et al., 2022).

In conclusion, the legal and ethical implications of encryption backdoors are vast and multifaceted, touching on issues of privacy, security, and the role of government in regulating digital technologies. International legal frameworks such as the GDPR and the CLOUD Act provide important insights into the competing interests of privacy and security, while ethical considerations continue to provoke heated debate about the limits of government power and the rights of individuals. Legal precedents, including high-profile cases such as the Apple-FBI dispute, have further shaped the discourse, highlighting the complexities of balancing national security concerns with the fundamental right to privacy. As encryption continues to play a pivotal role in safeguarding personal data, the debate over backdoors is likely to remain a critical issue for policymakers, legal experts, and the public at large. The challenge will be to find a balance that protects both national security and individual privacy, without compromising the integrity of digital security systems or eroding fundamental human rights.

6. Global Approaches to Encryption and Cybersecurity Policy

The global landscape of encryption and cybersecurity policy is marked by divergent approaches, with countries adopting varying strategies based on their national security priorities, privacy concerns, and geopolitical considerations. These differences have led to complex debates regarding the use of encryption backdoors, with governments seeking to balance law enforcement needs with the protection of personal privacy. While encryption plays a central role in securing communications

and safeguarding data, it also presents challenges for governments who wish to monitor potential security threats. Countries such as the United States, the United Kingdom, China, and members of the European Union have all taken unique stances on the issue of encryption, reflecting the broader geopolitical and legal contexts in which they operate.

In the United States, the debate over encryption backdoors has been particularly contentious. On one hand, US law enforcement agencies have long advocated for the ability to access encrypted data as part of criminal investigations and counterterrorism efforts. This stance has been supported by various pieces of legislation, such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which allows US authorities to compel companies to provide access to encrypted data stored abroad. The CLOUD Act was passed in 2018 and has been a focal point of the debate surrounding cross-border data access, with proponents arguing that it facilitates international cooperation in criminal investigations (Chandravathi, 2018). However, this approach has been met with strong opposition from technology companies, civil liberties groups, and privacy advocates who argue that creating backdoors would undermine the security of encryption systems and expose individuals' data to potential abuse. The high-profile legal battle between law enforcement agencies and technology companies, such as the FBI-Apple encryption dispute, further exemplifies the tension between national security and personal privacy. In this case, the FBI sought access to an encrypted iPhone used by a suspect in a terrorist attack, while Apple resisted, arguing that creating a backdoor would set a dangerous precedent for security and privacy (Abu-Salma, Krol, et al., 2017; Abu-Salma, Sasse, et al., 2017).

The United Kingdom has taken a somewhat similar approach to encryption backdoors, though with a more explicit focus on state surveillance. The UK's Investigatory Powers Act, often referred to as the "Snooper's Charter," grants law enforcement agencies the power to compel telecommunications companies to provide access to encrypted data. This law, passed in 2016, has been described as one of the most expansive surveillance laws in the Western world. It requires companies to provide "technical capabilities" to assist in the interception and decryption of communications when authorized by a warrant (Cheng & Zhang, 2014). Critics argue that this law undermines personal privacy and could lead to an erosion of trust in the digital economy, as individuals may fear their communications and data are being surveilled by government agencies. The UK's approach emphasizes a balance between the need for law enforcement to access encrypted data and the protection of national security, though it has been met with significant criticism both domestically and internationally for potentially infringing upon fundamental privacy rights (Abu-Salma, Krol, et al., 2017; Abu-Salma, Sasse, et al., 2017).

In contrast, China has adopted a much more restrictive approach when it comes to encryption and cybersecurity. The Chinese government has prioritized state control over the flow of information, which includes the use of encryption technologies to protect sensitive government data and communications while also implementing stringent regulations that enable the government to access encrypted information for national security purposes. China's 2017 Encryption Law requires all encryption systems used in the country to be vetted and authorized by the government, and it mandates that companies hand over access to encrypted communications upon request. The Chinese government has argued that such regulations are necessary to safeguard national security and protect against cyber threats, particularly as the country faces challenges related to cyber-espionage and cyberattacks (Chen et al., 2019). However, the extensive government surveillance and censorship mechanisms employed in China have raised serious concerns among human rights organizations, who view these practices as oppressive and a violation of personal privacy. The country's approach highlights the tension between securing national borders and controlling information, at the expense of individual freedoms (Cheng & Zhang, 2014).

In the European Union, the stance on encryption is more nuanced, reflecting a stronger emphasis on privacy protection. The General Data Protection Regulation (GDPR), which came into effect in 2018, places a high value on protecting the privacy and data security of individuals. The regulation explicitly encourages the use of encryption to protect personal data, particularly for organizations handling sensitive information. However, the GDPR also provides exceptions for access by law enforcement agencies in specific circumstances, such as when there is a legitimate reason tied to national security or criminal investigations. This has led to an ongoing debate within the EU about the balance between encryption for privacy and the need for lawful access to data (Chandravathi, 2018). The EU's approach is somewhat aligned with the notion that strong encryption is necessary for securing personal data, but at the same time, law enforcement must be able to access that data under certain conditions to ensure public safety. This delicate balance creates challenges for policymakers, as they seek to respect privacy rights while addressing security concerns.

These differing national approaches to encryption and the use of backdoors are not merely theoretical; they have significant implications for international cooperation and conflict. Countries with divergent policies on encryption may find it difficult to collaborate on cybersecurity matters, particularly when dealing with cross-border cybercrime, terrorism, or cyber-espionage. For instance, the US's aggressive stance on cross-border data access through the CLOUD Act has been criticized by the European Union, which prioritizes privacy and data protection under the GDPR. Similarly, China's strict surveillance laws and requirements for government access to encrypted data have led to tension with international organizations and foreign governments concerned about the broader implications of such policies on global cybersecurity norms (Chandravathi, 2018). These conflicts can complicate efforts to coordinate on matters like the investigation of cyberattacks or the regulation of global digital platforms.

International cooperation on cybersecurity is often hindered by the differences in national policies regarding encryption. The US's push for backdoors to encrypted data, for example, conflicts with the EU's stance on data privacy, leading to potential diplomatic and legal challenges. This divergence has led to a patchwork of national regulations that complicate global efforts to combat cybercrime and maintain secure digital environments (Chen et al., 2019). While international organizations such as the United Nations and the European Union have attempted to foster global norms for cybersecurity and encryption, these efforts have often been undermined by the conflicting interests of major global powers.

International organizations like the United Nations and the European Union play a crucial role in shaping global cybersecurity norms related to encryption. The UN has worked to develop international standards for cybercrime, including initiatives aimed at fostering cooperation between member states to address cross-border digital crimes. The UN's initiatives, however, often face challenges due to the competing interests of member states with differing priorities on encryption and data privacy (Chen et al., 2019). Meanwhile, the European Union has sought to establish itself as a leader in privacy protection, emphasizing the role of encryption in securing data in a way that protects individual freedoms. The EU's GDPR has set a strong example of how a regional framework can influence global privacy standards, though its impact on global encryption policies remains mixed due to the resistance of countries like the US and China (Chandravathi, 2018).

Despite these efforts, there remains a significant gap in the development of a unified global approach to encryption and cybersecurity. As national policies continue to evolve, international dialogue and collaboration will be essential to addressing the ongoing challenges posed by encryption, cybersecurity, and the protection of personal privacy. The future of global cybersecurity will likely depend on the ability of countries and international organizations to reconcile divergent approaches to encryption and create frameworks that can balance national security needs with the protection of fundamental human rights.

7. Challenges in Balancing National Security and Personal Privacy

The challenge of balancing national security with personal privacy is especially pronounced when it comes to encryption and the potential for creating backdoors. Governments, law enforcement agencies, and technology companies all have a vested interest in how this balance is struck, but finding common ground is not straightforward. Several key challenges complicate the efforts to harmonize these concerns, including technical difficulties in implementing encryption backdoors, policy and governance challenges in establishing international regulations, and the role of public perception and trust.

One of the most significant technical difficulties in implementing encryption backdoors lies in the inherent vulnerabilities they introduce into systems designed to be secure. Encryption works by converting data into an unreadable format that can only be deciphered using a decryption key. This cryptographic security is designed to protect sensitive information from unauthorized access. A backdoor, however, would introduce a deliberate vulnerability into this system, allowing authorized parties (such as government agencies) to access the encrypted data. The primary issue is that this "weakness" would not only be available to authorized parties but could also potentially be exploited by malicious actors.

Once a backdoor is created, it becomes a target for hackers, cybercriminals, or other malicious entities. These actors may attempt to discover and exploit the backdoor for their own purposes, leading to a significant security breach. For example, if a backdoor is introduced in a widely used encryption system, the entire user base of that system could be at risk. The risk of exploitation is particularly concerning for sensitive data, such as personal financial information or state secrets. Additionally, the process of creating backdoors may not be as straightforward as it seems. Cryptographic systems are often highly complex, and introducing even small changes can have unintended consequences on the system's overall security. This complexity is

one reason why security experts and encryption providers strongly oppose backdoor implementation, fearing that the potential harm far outweighs any perceived benefits in terms of national security (Chen et al., 2019).

Creating international policies that balance national security with personal privacy poses significant governance challenges. Countries vary widely in their legal, political, and cultural approaches to both encryption and privacy. While some nations prioritize individual privacy and civil liberties, others place more emphasis on national security and law enforcement. This divergence creates difficulties when attempting to create uniform, international standards on encryption and backdoors.

One of the major issues is the question of enforcement and compliance. Even when international agreements or regulations are formed, different countries may interpret or implement them in various ways. For instance, the European Union has stringent regulations like the General Data Protection Regulation (GDPR), which places high value on protecting individuals' privacy through encryption. However, many other jurisdictions, particularly those outside the EU, have far less robust privacy protections, and enforcement of international agreements is often inconsistent. This divergence in policies creates a patchwork of regulations and makes it difficult to ensure that encryption backdoors, if allowed, do not become tools for widespread surveillance or cyber espionage (Cheng & Zhang, 2014).

The challenge of enforcing international standards is further complicated by the rapid pace of technological advancements. New encryption methods are constantly being developed, and the legal frameworks often struggle to keep up with technological progress. Moreover, countries that do not participate in international agreements, such as authoritarian regimes, may introduce their own national encryption policies, sometimes bypassing international norms entirely. This inconsistency can create legal and diplomatic tensions, as countries with differing priorities may clash over the control of data and encryption technologies (Curtmola et al., 2011).

Public perception and trust in government decisions around encryption and privacy play a crucial role in shaping policy. In democracies, the government is supposed to represent the interests of its citizens, yet public sentiment toward surveillance and privacy varies significantly. Many citizens view encryption as an essential protection against the erosion of personal freedoms, while others worry that strong encryption can be used to shield criminal activity. When governments propose legislation to introduce encryption backdoors, they often face backlash from the public, who view these measures as an invasion of privacy. These concerns are amplified when there is a lack of transparency or accountability in government actions (Abu-Salma, Krol, et al., 2017; Abu-Salma, Sasse, et al., 2017).

Trust in technology companies is also a critical factor. Users of encrypted communication platforms generally expect their data to be protected from unauthorized access, and companies that fail to protect privacy can face significant reputational damage. When these companies comply with government requests to insert backdoors, it often leads to a loss of trust among their user bases. The lack of a clear and coherent policy from governments regarding how backdoors will be implemented, who controls them, and how they will be safeguarded can result in widespread public skepticism and undermine confidence in both governmental and corporate actors (Abu-Salma, Krol, et al., 2017; Abu-Salma, Sasse, et al., 2017).

The role of public opinion in shaping encryption policy underscores the need for transparency in decision-making and a deeper conversation about the trade-offs between privacy and security. Without clear communication, the public may perceive the implementation of encryption backdoors as an overreach of government power, potentially eroding trust in both democratic institutions and technological systems.

8. Future Directions and Recommendations

As the debate over encryption backdoors continues to evolve, innovative solutions must be explored to find a middle ground between security and privacy. Both technological advancements and policy innovations offer potential pathways for reconciling these two priorities, though challenges remain. In the pursuit of a balanced approach, key considerations include finding technological solutions that address national security concerns without undermining personal privacy, as well as crafting policy frameworks that can be effectively implemented across jurisdictions.

One potential technological solution to address the encryption-backdoor dilemma is the development of end-to-end encryption systems that allow for lawful access mechanisms under strict legal oversight. These systems could enable law enforcement agencies to access encrypted data when necessary, but only under carefully controlled conditions that prevent

unauthorized use. For example, a framework could be established in which encrypted data can be decrypted only after a court order or with oversight from an independent body. Such solutions would need to ensure that encryption is not compromised in a way that exposes all users to risk but instead provides a mechanism for authorized access in targeted cases. One approach could involve the use of "key escrow" systems, where the decryption key is stored in a secure, regulated environment and can only be accessed through legal means. This would maintain the overall integrity of encryption while allowing for lawful access in critical situations, though it would still require substantial safeguards to prevent misuse (Cheng & Zhang, 2014).

Legally, governments can create stronger international norms around encryption and backdoors by engaging in multilateral dialogues aimed at crafting frameworks that balance privacy and security. These frameworks could be based on clear guidelines about when and how backdoors are permissible, with stringent controls to prevent misuse. Such international agreements could take into account different national priorities but also insist on transparency, accountability, and safeguards to protect citizens' privacy. Mechanisms for cross-border cooperation and information sharing, with strict legal oversight, could help avoid the fragmentation of global encryption policy and reduce tensions between countries with conflicting legal standards (Chen et al., 2019).

To address the ongoing encryption debate, policymakers must take a nuanced approach that considers the concerns of all stakeholders: national security agencies, technology companies, and privacy advocates. First, the legal frameworks governing encryption must be more transparent, with clear guidelines for when encryption backdoors may be used and how they are to be regulated. Governments should work with tech companies and cybersecurity experts to ensure that backdoors do not create systemic vulnerabilities that can be exploited by malicious actors. Laws should mandate strict oversight and accountability in the use of encryption backdoors, with regular audits and checks to ensure compliance with legal standards. Additionally, international bodies such as the United Nations or the European Union can play a key role in developing global standards for encryption policies, ensuring that privacy protections are maintained while providing law enforcement with the tools they need to address security threats.

The involvement of the tech industry is also crucial in developing technologies that provide security without compromising privacy. Tech companies should work to develop solutions that allow for lawful access to encrypted data without weakening encryption or creating vulnerabilities that can be exploited. Engaging with privacy advocates and national security agencies in a collaborative manner can help create innovative solutions that meet the needs of both parties.

9. Conclusion

The ongoing debate over encryption backdoors and the balance between national security and personal privacy represents one of the most challenging issues of our time. As digital technologies continue to evolve and permeate all aspects of society, the need for robust cybersecurity measures has never been greater. Encryption serves as a fundamental tool for securing sensitive information, protecting individuals' privacy, and enabling the digital economy to function securely. However, this essential technology has also become a focal point in the global debate on how to protect national security while safeguarding individual rights.

The legal, technical, and ethical implications of encryption backdoors are vast and complex. On the one hand, governments argue that encryption backdoors are necessary to combat cybercrime, terrorism, and other security threats. They believe that access to encrypted data is crucial for effective law enforcement and intelligence operations, especially in an age where criminals and terrorist organizations exploit secure communications to operate under the radar. On the other hand, the introduction of backdoors into encryption systems raises serious concerns about the erosion of personal privacy and the potential for misuse. Such vulnerabilities could expose sensitive data to exploitation by malicious actors, creating a significant risk to both individuals and institutions.

International legal frameworks, such as the General Data Protection Regulation (GDPR) in the European Union and the CLOUD Act in the United States, highlight the growing tension between the need for security and the protection of privacy. While these laws seek to address issues of data protection and access, they also underscore the challenges of creating effective global policies that respect both privacy rights and national security concerns. Divergent approaches to encryption by countries like the US, the UK, China, and EU members illustrate the complexities of finding a unified stance on the issue. The lack of a

global consensus is further compounded by the differing priorities and values of various governments, leading to conflicts and challenges in international cooperation.

The technical challenges of implementing encryption backdoors are also a major consideration. The introduction of backdoors inherently weakens the security of encryption systems, making them vulnerable to exploitation by cybercriminals and hostile nation-states. These risks cannot be ignored, as the potential consequences of widespread data breaches and cyberattacks are immense. Furthermore, the ethical implications of creating such vulnerabilities raise concerns about the loss of trust in digital systems. If individuals and organizations believe that their communications and data are not secure, the very foundation of the digital economy could be undermined.

Ultimately, the challenge lies in finding a way to balance the needs of national security with the rights of individuals to privacy and data protection. This requires innovative solutions that address both the technological and policy dimensions of the issue. Proposals such as end-to-end encryption with legal oversight, or lawful access mechanisms that allow authorities to obtain encrypted data in specific circumstances without compromising overall security, offer a potential middle ground. However, these solutions must be carefully designed to prevent abuse and ensure that any access to encrypted data is conducted in a transparent and accountable manner.

Moving forward, the dialogue between privacy advocates, national security agencies, and the tech industry must be ongoing and constructive. It is crucial that lawmakers, cybersecurity experts, and international bodies work together to develop frameworks that can provide security without compromising privacy. As technology continues to evolve, so too must our approach to these critical issues. It is only through collaboration, transparency, and a commitment to protecting both security and individual rights that we can navigate the complexities of encryption and cybersecurity in the 21st century. The future of digital privacy and security depends on our ability to strike a balance that respects the rights of individuals while ensuring the safety and stability of nations.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abu-Salma, R., Krol, K., Parkin, S., Koh, Kwan, K., Mahboob, J., Traboulsi, Z., & Sasse, M. A. (2017). The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. https://doi.org/10.14722/eurousec.2017.23006

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the Adoption of Secure Communication Tools. 137-153. https://doi.org/10.1109/sp.2017.65

Chandravathi, D. (2018). Performance Analysis of Homomorphic Encryption Algorithms for Cloud Data Security. *International Journal for Research in Applied Science and Engineering Technology*, *6*(3), 1589-1592. https://doi.org/10.22214/ijraset.2018.3243

Chen, L., Zhang, Q., Ma, J., & Li, K. (2019). Research on Neural Network Chaotic Encryption Algorithm in Wireless Network Security Communication. *Eurasip Journal on Wireless Communications and Networking*, *2019*(1). https://doi.org/10.1186/s13638-019-1476-3

Cheng, R., & Zhang, F. (2014). Obfuscation for Multi-use Re-encryption and Its Application in Cloud Computing. *Concurrency and Computation Practice and Experience*, *27*(8), 2170-2190. https://doi.org/10.1002/cpe.3399

Curtmola, R., Garay, J. A., Kamara, S., & Ostrovsky, R. (2011). Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. *Journal of Computer Security*, *19*(5), 895-934. https://doi.org/10.3233/jcs-2011-0426

Distler, V., Lallemand, C., & Koenig, V. (2020). Making Encryption Feel Secure: Investigating How Descriptions of Encryption Impact Perceived Security. 220-229. https://doi.org/10.1109/eurospw51379.2020.00037

Endeley, R. E. (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*, *09*(01), 95-99. https://doi.org/10.4236/jis.2018.91008

Hasanova, H., Baek, U.-J., Mu-gon, S., Cho, K., & Kim, M.-S. (2019). A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures. *International Journal of Network Management*, *29*(2). https://doi.org/10.1002/nem.2060

Hidayat, T., & Mahardiko, R. (2020). A Systematic Literature Review Method on AES Algorithm for Data Sharing Encryption on Cloud Computing. *International Journal of Artificial Intelligence Research*, *4*(1). https://doi.org/10.29099/ijair.v4i1.154

Kerschbaum, F., & Härterich, M. (2017). Searchable Encryption to Reduce Encryption Degradation in Adjustably Encrypted Databases. 325-336. https://doi.org/10.1007/978-3-319-61176-1_18

Kumar, A., Anandhi, T., & Muthu, R. (2017). Analysis of Pixel Merging for Multi Image Integration for Security Enhancement. *International Journal of Computer Applications*, *179*(4), 6-11. https://doi.org/10.5120/ijca2017915915

Kumar, M., Agrawal, A., & Garg, A. (2014). An Image Encryption Technique Based on Concatenating Images of Same Dimensions. *International Journal of Computer Applications*, *98*(14), 30-34. https://doi.org/10.5120/17253-7595

Kumar, M., & Chahal, A. (2014). Effect of Encryption Technique and Size of Image on Correlation Coefficient in Encrypted Image. *International Journal of Computer Applications*, *97*(12), 23-27. https://doi.org/10.5120/17059-7443

Li, D., Wu, J., Liang, Z. H., Li, L. Y., Dong, X., Chen, S. K., Fu, T., Wang, X., Wang, Y. Z., & Song, F. (2022). Sophisticated Yet Convenient Information Encryption/Decryption Based on Synergistically Time-/Temperature-Resolved Photonic Inks. *Advanced Science*, *10*(5). https://doi.org/10.1002/advs.202206290

Li, Z., Wang, X., Lin, Y., & Cheng, C. (2015). RDEA: A Novel Video Encryption Algorithm. 183-189. https://doi.org/10.1007/978-3-662-47487-7_28

Liu, Y. B., & Ren, W. (2013). Attribute-Based Authentication Protocol of the Internet of Things. *Advanced Materials Research*, *765-767*, 1726-1729. https://doi.org/10.4028/www.scientific.net/amr.765-767.1726

Nanda, A., Nanda, P., He, X., Jamdagni, A., & Puthal, D. (2020). A Hybrid Encryption Technique for Secure-Glor: The Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Networks. *Future Generation Computer Systems*, *109*, 521-530. https://doi.org/10.1016/j.future.2018.05.065

Nojeim, G., & Maheshwari, N. (2021). Encryption in India: Preserving the Online Engine of Privacy, Free Expression, Security, and Economic Growth. *Indian Journal of Law and Technology*, *17*(1). https://doi.org/10.55496/hgck9762

Popa, R. A., Li, F. H., & Zeldovich, N. (2013). An Ideal-Security Protocol for Order-Preserving Encoding. https://doi.org/10.1109/sp.2013.38

Rodriguez, S., & Centonze, P. (2017). Multi-Layered Dynamic Encryption Security Scheme for Cloud Data Storage. *International Journal of Computers & Technology*, *16*(3), 6233-6239. https://doi.org/10.24297/ijct.v16i3.6150

Şahin, M. F., Mahmood, M. K., & Myderrizi, I. (2020). Secure and Fast Encryption Routine+: Evaluation by Software Application. *International Journal of Engineering Technologies Ijet*, *6*(2), 13-24. https://doi.org/10.19072/ijet.755570

Samir, E. A., & Raissouni, N. (2019). CompactRIO Based Real Time Implementation of AES Algorithm for Embedded Applications. *International Journal of Embedded and Real-Time Communication Systems*, *10*(2), 19-36. https://doi.org/10.4018/ijertcs.2019040102

Samiullah, M., Aslam, W., Khan, M. A., Alshahrani, H. M., Mahgoub, H., Abdullah, A. M., Ullah, M., & Chen, C. M. (2022). Rating of Modern Color Image Cryptography: A Next-Generation Computing Perspective. *Wireless Communications and Mobile Computing*, *2022*, 1-20. https://doi.org/10.1155/2022/7277992

Shi, T., Hu, B., Guan, J., & Wang, S. (2022). Cryptanalysis of AEGIS-128. *Chinese Journal of Electronics*, *31*(2), 285-292. https://doi.org/10.1049/cje.2020.00.231

Spinello, R. A. (2020). The Ethical Consequences of "Going Dark". *Business Ethics the Environment & Responsibility*, *30*(1), 116-126. https://doi.org/10.1111/beer.12313

Taramonli, S., Green, R. J., & Leeson, M. S. (2012). Energy Conscious Adaptive Security Scheme for Optical Wireless. 1-4. https://doi.org/10.1109/icton.2012.6253913

Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. *International Journal of Advanced Computer Science and Applications*, *8*(1). https://doi.org/10.14569/ijacsa.2017.080151

Watzlaf, V. J., Moeini, S., Matusow, L., & Firouzan, P. (2011). VOIP for Telerehabilitation: A Risk Analysis for Privacy, Security and HIPAA Compliance: Part II. *International Journal of Telerehabilitation*. https://doi.org/10.5195/ijt.2011.6070

Yang, Y., Xiao, X., Cai, X., & Zhang, W. (2019). A Secure and High Visual-Quality Framework for Medical Images by Contrast-Enhancement Reversible Data Hiding and Homomorphic Encryption. *IEEE Access*, *7*, 96900-96911. https://doi.org/10.1109/access.2019.2929298

Yasser, I., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2020). A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications. *Entropy*, *22*(11), 1253. https://doi.org/10.3390/e22111253

Yazdeen, A. A., Zeebaree, S. R. M., Sadeeq, M. M., Kak, S. F., Ahmed, O. M., & Zebari, R. R. (2021). FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review. *Qubahan Academic Journal*, *1*(2), 8-16. https://doi.org/10.48161/qaj.v1n2a38