

Article

A Modern Approach to Securing Critical Infrastructure in Energy Transmission Networks: Integration of Cryptographic Mechanisms and Biometric Data

Anna Manowska ^{1,*} , Martin Boros ² , Muhammad Waqar Hassan ¹ , Anna Bluszcz ³
and Katarzyna Tobór-Osadnik ³ 

¹ Department of Automatics and Industrial Informatics, Silesian University of Technology, 44-100 Gliwice, Poland; muhammad.waqar.hassan@polsl.pl

² Department of Security Management, Faculty of Security Engineering, University of Žilina, 010-26 Žilina, Slovakia; martin.boros@uniza.sk

³ Department of Safety Engineering, Silesian University of Technology, 44-100 Gliwice, Poland; anna.bluszcz@polsl.pl (A.B.); katarzyna.tobor-osadnik@polsl.pl (K.T.-O.)

* Correspondence: anna.manowska@polsl.pl

Abstract: Energy security is a crucial issue for political, environmental, and economic reasons. This article presents a modern approach to securing critical infrastructure in energy transmission networks, which are managed by advanced IT systems. This paper focuses on the integration of cryptographic mechanisms with biometric data, providing an additional layer of protection against cyber threats. The discussed solutions enable the protection of management systems in energy transmission networks, enhancing their resilience to cyberattacks. The use of the command-line interface (CLI) in combination with biometrics allows for precise execution of security tasks such as network monitoring, firewall management, and automation of security tasks. This makes these systems more reliable and secure, which is essential for the stability of energy systems.

Keywords: energy security; critical infrastructure; energy transmission networks; cryptographic mechanisms; biometric data; cybersecurity; IT system management



Citation: Manowska, A.; Boros, M.; Hassan, M.W.; Bluszcz, A.; Tobór-Osadnik, K. A Modern Approach to Securing Critical Infrastructure in Energy Transmission Networks: Integration of Cryptographic Mechanisms and Biometric Data. *Electronics* **2024**, *13*, 2849. <https://doi.org/10.3390/electronics13142849>

Academic Editor: Libao Shi

Received: 2 July 2024

Revised: 13 July 2024

Accepted: 17 July 2024

Published: 19 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Fuel and energy management is associated with technical and economic risks. Technical risk should be understood as a specific probability of occurrence of a threat to humans and the technical and natural environment. The probability of an economic hazard determines the economic risk. These risks significantly impact the country's energy security. Both failures and the poor financial situation of energy companies significantly reduce the certainty of securing the energy needs of consumers, and this also determines the reduction in the level of energy security of the country [1,2].

The energy sector encompasses global markets, international economies, and various geopolitical environments. Therefore, this sector is not immune to emerging threats. But that does not mean it should not be ready to face these critical issues as they arise.

In the energy sector, where technical and economic risks are commonplace, it is crucial to manage risks related not only to physical infrastructure but also to digital security. As the sector becomes increasingly dependent on advanced information systems, the importance of cybersecurity is growing at an unprecedented rate. A cyberattack can cripple critical management systems, leading to catastrophic consequences on both a local and global scale. In the context of changing threats, which include global warming, changing regulations and technological innovations, cybersecurity is becoming the foundation for ensuring the continuity and stability of energy supply. Thus, the protection of IT systems against cyberattacks is an indispensable element of broadly understood energy security.

The most important threats that are currently affecting the energy sector are global warming and climate change, rapidly changing industry, cyber threats, tariffs and trade stress, and the labor market and catastrophic events.

Global warming and climate change are factors that have a strong impact on the energy sector. Emissions from fossil fuels are considered to be one of the main causes of the greenhouse effect. About 80% of the world's primary energy production comes from these fuels. The energy sector is making every effort to reduce emissions from hard coal and lignite. This is evidenced by the current level of electricity consumption from fossil fuels, which is the lowest since 1994. The sector invests in efficient combustion technologies and clean coal technologies. Despite these actions, there is strong pressure to further develop energy production. The energy sector must keep up with these changes and face a decline in demand.

Another risk facing the energy industry is the rapidly changing industry. This includes the development of renewable energy, the replacement of coal fuels with gas, and the evolution of the energy market structure. This can lead to a lot of unnecessary investment.

Energy companies are also investing in grid modernization, moving from mechanical to digital systems [3,4]. In the long run, this will have a positive impact on the industry, bringing it into the digital age. However, this transformation generates new threats, such as cyberattacks. In the digital world, there are many opportunities to access systems. Customers are using a variety of ways to connect in their homes, using smart devices that are part of a global network [5–7]. Hackers have more devices and access points to critical infrastructure.

The security of energy supply systems is a key element in ensuring the stability and reliability of critical infrastructure in the European Union countries. Developing effective strategies to protect these systems is an integral part of the plans to protect these infrastructures. Vulnerability analysis of these systems is necessary to build scenarios for preventive actions. In particular, attention should be paid to service providers and supply chain elements that may be weak links. A lack of knowledge and awareness within the team can also lead to potential security vulnerabilities. These areas require special monitoring to identify potential attack “gates”.

One of the effective solutions to strengthen security is the use of biometrics in combination with public key infrastructure (PKI) [8]. The use of hardware security modules (HSMs) further enhances protection by storing cryptographic keys in tamper-proof devices. HSMs manage and protect keys from theft or misuse, significantly reducing the vulnerability of critical infrastructure to cyberattacks.

An example of a serious security breach was the situation in Ukraine in 2015, when a cyberattack deprived about 230,000 consumers of access to electricity [9]. In this case, advanced tactics, techniques, and tools, including social engineering (phishing), were used to deliver BlackEnergy malware to the operator's network. Then, the attackers infiltrated the OT network and remotely shut down the power substations. In the final phase, software such as KillDisk was used, which made it impossible to work on workstations, and modifications to automation components, limiting the possibility of remote access.

Another example is the espionage campaign against the U.S. power distribution network, which ran from 2019 to 2020. The attackers tried to break into many accounts with weak passwords on a massive scale. Fortunately, these activities were detected by Microsoft before the attackers made their way from the IT network to the OT, which prevented more serious consequences [10].

Given how quickly cybercriminals exploit new vulnerabilities, even the most robust and resource-equipped security teams struggle to keep up with them. According to Skybox Research, a new security vulnerability is released every 17 min [11]. Given the rapid development of the cybercrime industry, it is important for specialists to be aware of the current state when creating attack schemes on IT systems. However, unfortunately, many security teams are constrained by outdated tools, staff shortages, and increasing regulatory requirements, so they struggle to understand and prioritize the most critical risks. Only a

proactive approach to security can help identify and stop cyber threats, while streamlining work and relieving staff workload, as shown in Figure 1.

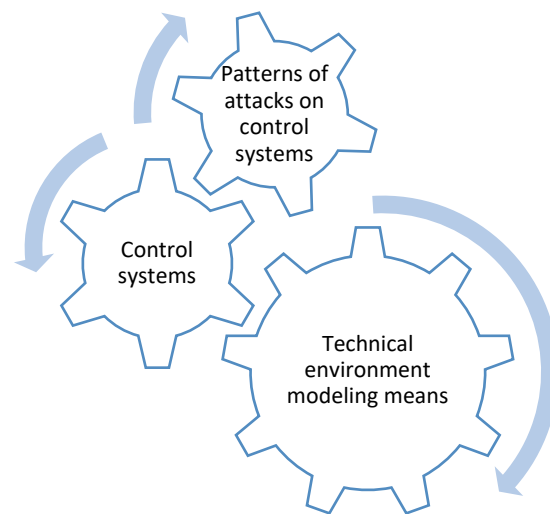


Figure 1. A proactive approach to security, source: own study.

The European Union is working to create a single legal framework to build resilient CI in the area of cybersecurity. On 14 December 2022, Directive (EU) 2022/2555 of the European Parliament and of the council concerning measures for a high common level of cybersecurity in the union, amending Regulation (EU) No 910/2014 [12,13] and Directive (EU) 2018/1972 were amended and repealing Directive (EU) 2016/1148 [14], was issued. This directive on measures for a high common level of cybersecurity in the Union: the so-called NIS 2 Directive is an amendment to the NIS Directive, the first European piece of legislation on cybersecurity. The NIS2 Directive combines the provisions on the protection of CI and the security of network and information systems. In addition, Directive 2022/2557 requires member states to adopt a strategy for increasing the resilience of critical entities by 17 January 2026.

2. Methodology

Today's governance of the energy sector requires taking into account all of the above-mentioned risks. This sector is strongly linked to an open multi-market economy and increasing competition. In the management of this sector, the importance of developing strategies based on the identification of threats, risk assessment, and the implementation of rational decisions over time, including technical solutions conducive to risk reduction in the most effective way, is growing.

The most difficult and fastest-growing threat is cyberattacks. The cyberattackers repeatedly change their approach to bypass the deployed security mechanisms [7]. This complexity has attracted great attraction from researchers recently, and they are presenting algorithms to fulfill the necessary data-securing requirements [15–20].

This article adopts a research hypothesis that has been verified through literature analysis, computer simulation, and case studies to assess the potential benefits and limitations of biometric authentication mechanisms in the context of critical infrastructure management:

H0. *The implementation of biometric authentication mechanisms significantly improves the security and reliability of power transmission management systems compared to traditional authentication methods such as passwords.*

This article reviews the use of command-line interface in the context of managing the security of critical infrastructure information systems. The potential of integrating biometric

data with cryptographic mechanisms to meet challenges in this field was also analyzed. The next step examined how CLI can be used to implement and manage advanced security solutions with biometric authentication mechanisms.

3. An Overview of the Command Line as a Security Management Tool

The command-line interface is very vulnerable in the context of security management. Due to its control and simplicity, it is also superior to a graphical user interface (GUI). The administrator can use a precise command which works very fast and efficiently. Much of the literature shows the importance of CLIs in the field of cybersecurity.

In article [21], the author discusses how CLIs, a Unix-based system, are widely used and enhance security features. The role of CLIs in the implementation of security systems and management of network configuration to secure the IT environment is discussed. According to [22], the use of command-line interfaces is a basic skill for cybersecurity professionals. Many advanced security tools are designed in this way so that they can be operated with the help of a command line, and because they need precision and scriptability, which are not available in GUI tools.

In [23], a comprehensive overview and application of CLI are presented. The author discusses the importance of this tool and how this tool can be used in the monitoring of health and responses to incidents in a sophisticated way. This can be used in the encryption and decryption process with biometric systems for enhancing the security protocols as seen in [24]. In summary, this is a powerful tool for security management. This tool, with its precision and integration with the latest technology, makes it a suitable choice for the security of IT systems.

4. An Introduction to Biometrics and Their Role in Encryption

The measurement of human physiological and behavioral properties is referred to as biometrics. The biometrics traits are of two types. One is biological traits that include fingerprints, faces, and irises, while behavioral traits include voices, signatures, and keystrokes. Nowadays, security is a major concern, and to remove the old password system, many digital systems use biometric systems to enhance security. Data and system protection become the utmost priority.

Biometric encryption or bio-cryptography uses the biological traits of humans to secure encryption algorithms. The advantage of this system is that it can be only accessed by authorized persons. This also includes challenges because once the system is compromised, it cannot be replaced like a password.

In [25], a comprehensive review of biometric systems and their application is provided. The author also discusses the process of how biometric data can be captured, processed, and matched. In [26], the critical issue of biometric templates is discussed. Different biometric encryption techniques are discussed in [27]. Its author discusses how this can be used in cryptographic systems. In [28], the author discusses two-factor authentication which is very secure and reliable. Its literature review reports that biometric systems are secure and reliable; nevertheless, some issues require robust systems that will make data more secure.

5. Command Line in System Security Management

Interactions with systems can be carried out with direct and scriptable methods. In an IT system, to perform tasks with precision and accuracy, text-based interfaces are considered an optimal choice. The literature shows that CLIs play an important role in security management (Table 1).

The literature above emphasizes that the command line interface is the best tool for security management based on its applications. Their direct connection with systems enhances their security features.

Table 1. Literature review of CLIs in security management.

Sr No.	Role of CLIs	References
1	This paper discusses how CLIs enable the creation and execution of automated scripts which perform security checks. If this is performed manually, there is a chance for error.	[29]
2	In this paper, the use of CLIs in configuring firewalls and the management of network security systems are discussed with examples.	[30]
3	CLIs' role in system audits is discussed in this paper. This can be used to monitor system records and alert the system in case of any suspicious activity.	[31]
4	In this paper, tools like Nmap for security auditing are discussed. These tools are valuable because they can identify open ports and services.	[32]
5	This paper discusses how CLIs can be used with biometric systems to enhance security. It also discusses how command-line tools can be used to control data flow between biometric sensors.	[33]

5.1. Command-Line Tools for Various Operating Systems

5.1.1. Unix/Linux

This operating system is known for its strong set of command-line-interface tools. For searching text, `grep` is used. `Awk` is used for pattern scanning, and `sed` is used for stream editing. `Ls` is used for listing the directory. `Cp` is for copying files, and `mv` is used to rename a file or move a file. To check network connectivity, `ping` is used.

5.1.2. Windows

In the Windows operating system, there are different command prompts: `dir` is used to list files, `copy` is used for file duplication, and `del` is used for the deletion of files. With the help of Windows PowerShell, users experience a more convenient CLI environment. Advanced scripting can also be carried out with the help of PowerShell.

5.1.3. macOS

macOS is very similar to Unix/Linux. The same tools like `bash`, `zsh`, and `fish` are used. `Diskutil` is used for disk management, and `tmutil` is used for Time Machine backups. Users can also install the Homebrew package manager to install Unix applications on their systems.

6. Materials and Methods

6.1. Command-Line Approaches for Firewall Management and Network Monitoring

The EU legal framework of the General Data Protection Regulation and ePrivacy Regulation establishes a requirement for the protection of personal data and the security of information systems [34–37]. According to the regulations, organizational measures must be taken to ensure data security.

According to this, the command-line interface (CLI) is the best tool which ensures security [38,39]. The CLI can monitor network activity, firewall management, and automation with the help of scripting.

6.1.1. Monitoring Network Activity

Linux:

Administrators can capture and analyze network packets with the help of the *tcpdump* command.

```
SUDO TCPDUMP -I ETH0 P'ORT 80'
```

This command listens for traffic on port 80 (HTTP) on the eth0 interface. The output will show packets being sent to and from the server on this port.

Windows:

PowerShell offers a similar capability to Get-NetTCPConnection.

```
GET-NETTCPCONNECTION | WHERE-OBJECT { $_.LOCALPORT -EQ 80 }
```

This command filters current TCP connections to show those involving local port 80. The output lists active connections, including their statuses and remote addresses.

macOS:

On macOS, netstat can be used to monitor network connections.

```
NETSTAT -AN | GREP '.80'
```

This command displays all active connections to and from port 80. The output includes the protocol, address, and state of each connection.

6.1.2. Managing Firewalls

Linux: iptables is the go-to tool for configuring firewalls.

```
SUDO IPTABLES -A INPUT -P TCP --DPORT 22 -J ACCEPT
```

This script adds a rule to accept incoming SSH connections. There would be no output if the command executes successfully.

Windows:

The Windows Firewall can be managed with Netsh.

```
NETSH ADVFIREWALL FIREWALL ADD RULE NAME = "ALLOW SSH" DIR = IN ACTION = ALLOW  
PROTOCOL = TCP LOCALPORT = 22
```

This command creates a rule to allow inbound SSH connections to port 22. The output will confirm the creation of the rule.

macOS:

pfctl is used for firewall configurations.

```
(SUDO PFCTL -SR; ECHO "PASS IN PROTO TCP FROM ANY TO ANY PORT 22") | SUDO PFCTL -F -
```

This command adds a rule to allow SSH connections. The output from pfctl -sr would list the current set of rules before the new rule is added.

6.1.3. Automating Security Tasks with Scripts

Linux:

A simple bash script can automate the update process and scan for rootkits.

```
#!/BIN/BASH

ECHO "UPDATING SYSTEM AND CHECKING FOR ROOTKITS..."

SUDO APT-GET UPDATE && SUDO APT-GET UPGRADE -Y

SUDO RKHUNTER -CHECK
```

The output would show system updates being applied followed by the rootkit hunter's scan results.

Windows:

PowerShell can be used to automate security updates and scans.

```
WRITE-HOST "UPDATING SYSTEM AND CHECKING FOR MALWARE..."

START-PROCESS -FILEPATH "POWERSHELL" -ARGUMENTLIST "UPDATE-MPSIGNATURE" -WAIT

START-PROCESS -FILEPATH "POWERSHELL" -ARGUMENTLIST "START-MPSCAN -SCANTYPE
QUICKSCAN" -WAIT
```

The output would indicate the update of Windows Defender signatures and the completion of a quick malware scan.

macOS:

Automating tasks on macOS can be performed using a bash script with softwareupdate and clamscan.

```
#!/BIN/BASH

ECHO "UPDATING SYSTEM AND SCANNING FOR MALWARE..."

SUDO SOFTWAREUPDATE -IA && CLAMSCAN --INFECTED --REMOVE --RECURSIVE /USERS
```

The output would show the system updates being installed and the results of the ClamAV malware scan.

6.1.4. Detecting and Removing Malware

Linux:

ClamAV can be used to scan for and remove malware.

```
SUDO CLAMSCAN --INFECTED --REMOVE --RECURSIVE /HOME
```

The output would list infected files and their removal statuses.

Windows:

Windows Defender CLI can perform malware scans.

```
START-MPSCAN -SCANTYPE FULLSCAN
```

The output would show the progress and results of a full-system malware scan.

macOS:

ClamAV can also be used on macOS.

```
CLAMSCAN --INFECTED --REMOVE --RECURSIVE /USERS
```

The output would be similar to that of Linux, listing any detected malware and actions taken.

6.1.5. Analyzing Logs for Potential Threats

Linux:

grep can be used to search through log files.

```
GREP "FAILED PASSWORD" /VAR/LOG/AUTH.LOG
```

The output would show lines from the log file that contains failed password attempts, indicating possible unauthorized access attempts.

Windows:

PowerShell’s Get-WinEvent can filter event logs.

```
GET-WINEVENT -LOGNAME SECURITY | WHERE-OBJECT { $_.MESSAGE -MATCH "FAILED LOGON" }
```

The output would list security log entries related to failed logon attempts.

macOS:

grep can be used similarly to Linux.

```
GREP "AUTHENTICATION ERROR" /VAR/LOG/SYSTEM.LOG
```

The output would show log entries for authentication errors, which could suggest attempted breaches.

6.1.6. Effective Commands for System Security Audits

Linux:

lynis is a security auditing tool for Linux systems.

```
SUDO LYNIS AUDIT SYSTEM
```

The output would provide a security report with suggestions for improvements.

Windows:

Microsoft Baseline Security Analyzer (MBSA) can be used for security auditing.

```
MBSACLI /NVC /ND /WI /NVC
```

The output would include a list of vulnerabilities and misconfigurations.

macOS:

lynis can also be used on macOS.

```
SUDO LYNIS AUDIT SYSTEM
```

The output, as with Linux, would be a detailed security report.

These examples illustrate the versatility of command-line tools across different operating systems for maintaining system security.

6.2. Biometric Data in Encryption Processes

Biometric data are the unique physical and behavioral characteristics that can be used for automated recognition of individuals [40–45]:

1. Fingerprint Recognition: One of the oldest and most widely used biometric types, fingerprint recognition involves analyzing the ridges and valleys on the surface of a finger.
2. Facial Recognition: This technology maps facial features from a photograph or video and compares the information with a database of known faces.
3. Iris Scanning: Iris recognition uses the unique patterns of a person's iris to identify and authenticate their identity.

Each biometric type has its own set of difficulties and needs specific hardware and software to obtain and handle the data.

The incorporation of biometric data into encryption processes recommends several advantages [40–45]:

1. Improved Security: Biometric traits are naturally linked to an individual which are impossible to forge.
2. User Convenience: Biometrics can provide a seamless user experience, as there is no need to remember passwords or carry tokens.
3. Non-repudiation: Biometric systems can provide strong evidence for authentication, reducing the risk of repudiation.

However, this incorporation is not without its challenges [46–51]:

1. Privacy Concerns: The storing and use of biometric data raise considerable privacy issues, as biometric features are classified personal information.
2. Security of Biometric Data: If biometric data are compromised, it cannot be changed like a password, making storage secure and processing critical.
3. False Acceptance and Rejection: Biometric systems are not infallible and can mistakenly accept an unauthorized user or reject an authorized one.

Command-Line and Biometrics Integration

In the modern age of cybersecurity, the incorporation of biometric authentication with command-line interfaces (CLIs) represents a major leap forward in locking access to sensitive systems and data. Biometrics offer a unique layer of security based on personal attributes, such as fingerprints, facial recognition, and iris scans, which are difficult to replicate or steal.

The integration of biometrics with command lines enhances security protocols in different ways that are secure and reliable. The main aspects in which security will be enhanced are as follows:

- Seamless integration;
- Enhanced security;
- Multi-factor authentication (MFA);
- Automation and efficiency;
- Scalability;
- Privacy compliance;
- Error handling and logging;
- User feedback;
- Cross-platform compatibility.

7. Results

The “Bio Command Authenticator” algorithm was developed to increase the level of security of information systems by integrating users' biometric characteristics with cryptographic mechanisms.

This innovative algorithm uses unique, hard-to-forge biometric features such as fingerprints, facial recognition, and iris scanning. Each of these biometric features is highly

different, making it much more difficult for unauthorized people to gain access to protected system resources.

The mechanism of operation of the “Bio Command Authenticator” algorithm is as follows:

- **Biometric Download:** The process begins with the collection of biometrics from the user. Fingerprint scanning has been added to the developed algorithm, which results in the analysis of ridge and valley patterns on the surface of the finger. This is a biometric method which is characterized by high accuracy and a low probability of a false match.
- **Data Processing:** The biometric data collected is then processed and analyzed to extract distinctive features that are unique to each user.
- **Cryptographic Security:** Extracted biometric features are integrated into cryptographic algorithms. Biometric data are used to generate encryption keys, ensuring that only authorized users can decrypt and access protected information.
- **Verification:** Each time the user logs in, the user must provide their biometric data, which are compared with the previously registered data in the system. If the data match, the user is granted access to the system.

Analyzing the legal aspects on the basis of which the algorithm was developed and in accordance with the applicable Zero Trust principle, the organization’s resilience to ICT threats should include identity, data, software, infrastructure, applications, and networks. Identity protection should include strong user authentication, verification of devices used, verification of permissions (minimum, necessary, and temporary), and verification of activity (for anomalies, including, for example, data leaks or extractions). At the same time, the provisions on image and personal data protection should be taken into account. A block diagram is shown in Figure 2.

The concept of the system can be seen in the block diagram. This block diagram is iterative, which allows continuous improvement, and new biometric technologies can be added to this.

The step-by-step description of the algorithm is as follows:

1. Initialization: In the first step, the device is initialized. The calibration of the sensors and required actions are taken at this step.
2. Data Capture: The second step is the collection of biometric data.
3. Data Processing: These data are processed and analyzed. A preprocessing technique is applied to match the data with the database.
4. Data Matching: This step includes the verification of the data with the stored data.
5. Authentication Evaluation: After the matching, the authentication process starts. If it does not match, permission will not be granted.
6. Command-Line Execution: If the user is authorized, the command-line interface will be executed.
7. Logging: This step involves logging which is very necessary for security purposes.
8. Error Handling: The algorithm includes error handling.
9. Cleanup: After authentication, temporal data will be erased.
10. Security Checks: Regular security checks are conducted for the security checkup.
11. User Feedback: Feedback to the user is also provided.
12. Compliance and Privacy: Privacy and compliance are kept in mind while making this algorithm.

For biometric authentication, code is made in Python which is based on the structural similarity index between two images. A database containing images of fingerprints is available. This structural similarity index is used to compute the values between -1 and 1 based on contrast. The hash function is used to compute the SH-256 which will produce the 32-byte hash value which is known as message digest. XOR is used for encryption. The encryption data are returned. Then, the decryption function is used for decryption. Biometric feature extraction is used to obtain features from the biometric data. Then,

a similarity search is used to find similarities. The threshold set for the comparison of biometric data is 0.8%. If the similarity is greater than this, access is granted, and this will create an encryption key; otherwise, access will be denied. Algorithm 1 is as follows:

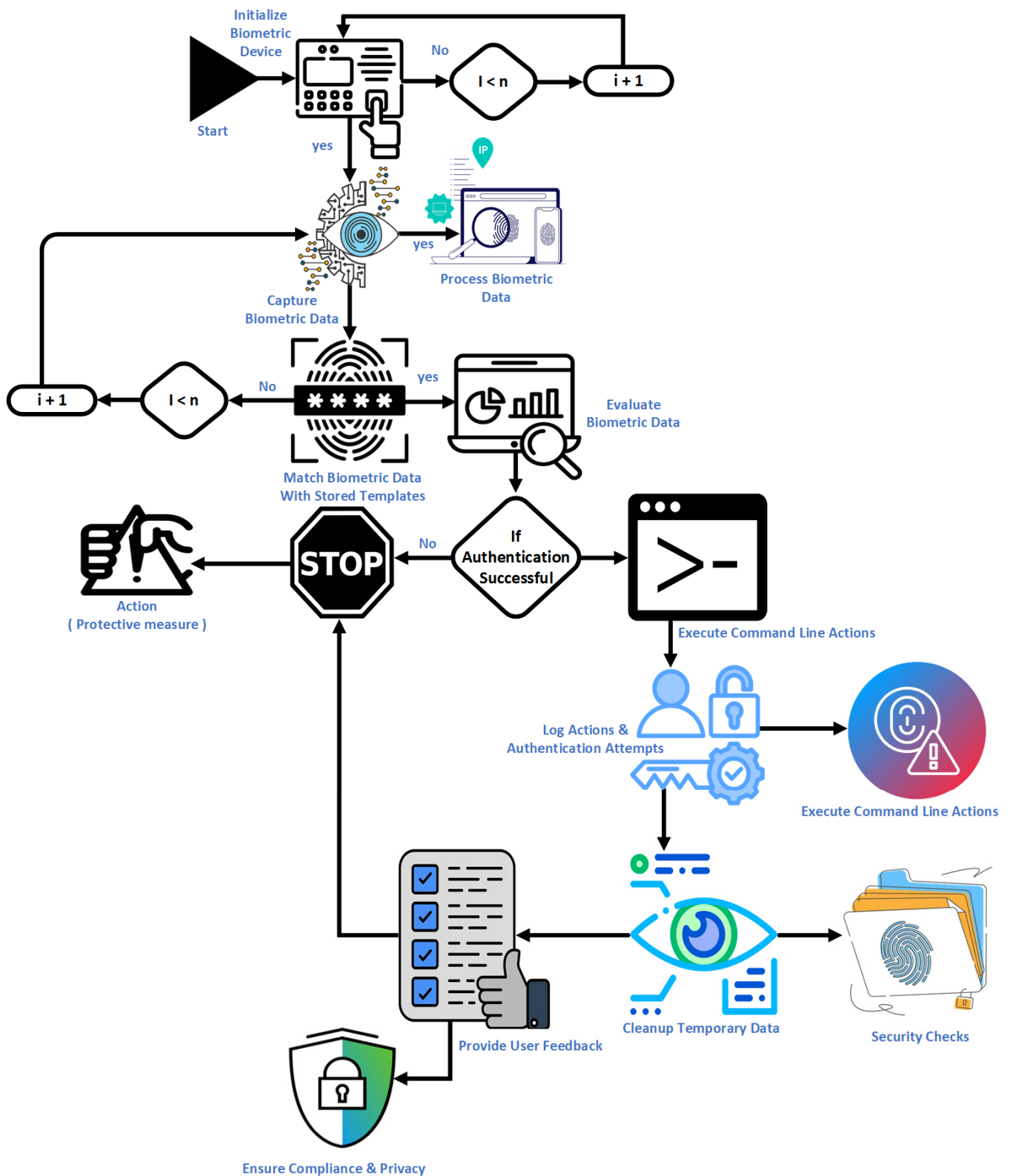


Figure 2. Bio Command Authenticator—block diagram, source: own study.

Algorithm 1: Proposed encryption key generation through biometric system for cryptography

```

1  Import Libraries: import (os, cv2, NumPy as np, HashLib)
2      Import image metrics and structural similarity
3      Function (read image)
4          Return (Image path through cv2)
5  Data Encryption
6      Function to extract data (Biometric features):
7          # Compute the hash of biometric data
8          Return (Biometric Data) //The encryption of the data will be done.
9      Function biometric-based encryption (Data, Biometric features):
10         Data encryption = bytes ([Data[i] ^ Biometric features [i % len (Biometric features)] for in range (len
(Data))])
11         Return (Encrypted Data)
12  Data Decryption
13      Function biometric-based decryption (Encrypted data, Biometric features):
14         Data decryption = bytes ([Encrypted data[i] ^ biometric features [i % len (Biometric features)] for
i in range (len (Encrypted data))])
15         Return (Decrypted Data) //Comparison of images and their features.
16      Function image comparison (Image A, Image B):
17          # Compute Structural Similarity Index
18          Score, _ = sim (image A, image B, full=True)
19          Return (Score)
20  Similarity Check
21      Function search similarity (Image, Reference biometric data):
22          # Extract biometric features from the reference image
23          Biometric features = Extract biometric features (Reference biometric data)
24          # Encrypt image data with biometric features
25          Biometric-based data encryption = Biometric encryption (Image to bytes (), Biometric
features)
26          # Decrypt the encrypted data with the same biometric features
27          Biometric-based data decryption = Biometric decryption (Encrypted biometric
data, Biometric features)
28          # Compute the similarity score of the image and decrypted data
29          Similarity score = Image comparison (Image, Buffer np (Decrypted biometric data,
type), Image reshapes (image. Shape))
30          Return (Similarity Score)
31  Similarity Check Based on Threshold Value
32      Function search similar image (Image path, folder path, threshold):
33          Query image = Read image (Image path)
34          For (folder path):
35              If (check the file name and extension):
36                  Image file = path join (folder path, filename)
37                  Reference image = Read image (image file)
38                  Similarity score = Compare images (Query image, Reference image)
39                  If (Similarity score > threshold):
40                      # If the similarity is above the threshold, return biometric features
and similarity score
41                      Biometric features = Extract biometric features (Reference image)
42                      Return (Biometric features, Similarity score)
43                      # If no similarity is found above the threshold, return None
44                      Return (None, None)
45  Comparison
46      If (Check name similarity):
47          Folder path
48          Image path
49          Encryption key, Similarity score = check similarity (Image path, Folder
path)
50          If (encryption key is not None):
51              Print (Similarity found, folder path, similarity score)
52              Print (Encryption Key)
53          Else:
54              Print (No similarity found with the images in the folder. Access
Denied)
55  Execution of Command Line (if permission is granted)

```

The biometric fingerprint images are stored in the database as shown in Figure 3. These images will be further used for comparisons. The features of each image are compared to the image of the input. Furthermore, the results of the comparison are shown in Figure 4.



Figure 3. Database of images, sources: own study.

```
[ ] if __name__ == '__main__':
    reference_biometric_data = b'SampleBiometricData123'
    image_path = '/content/11.jpg'
    access, score, encryption_key = biometric_security_system(image_path, reference_biometric_data)
    if access:
        print(f'Access Granted. Similarity Score: {score:.2f}')
        print(f'Encryption Key: {encryption_key.hex()}')
    else:
        print(f'Access Denied. Similarity Score: {score:.2f}')
```

```
Access Granted. Similarity Score: 1.00
Encryption Key: e95b81150ee4612d7fa97e3ffdb8a5b3b0bbffbf5fa283a9955f737b6ba54ca
```

Figure 4. Output of access granted and generation of encryption key, source: own study.

In Figure 4, the results are shown. First, the image of the biometric data is compared to the images that are in the database. Then, a comparison between the different biometric features is performed. If the biometric features are a match greater than 80%, access is granted, and an encryption key will be generated. In Figure 5, the fingerprint is compared with the database, but the image is not yet stored in the database. The score of the comparison of the features is less than 80%; this is why no similarity is found, and access is denied.

```
[ ] if __name__ == '__main__':
    access, score = biometric_security_system('/content/11.jpg', '/content/12.jpg')
    if access:
        print(f'Access Granted. Similarity Score: {score:.2f}')
    else:
        print(f'Access Denied. Similarity Score: {score:.2f}')
```

```
Access Denied. Similarity Score: 0.09
```

Figure 5. Output of access denied, source: own study.

8. Discussion

The “Bio Command Authenticator” algorithm has a significant impact on increasing the reliability and resilience of energy transmission management systems or other IT systems of critical infrastructure. The integration of biometric authentication mechanisms with energy transmission management systems not only improves the level of security, but also supports the continuity of these systems, which is crucial to ensure the stability of energy supply.

Biometric authentication ensures that only authorized operators can access energy transmission management systems. This eliminates the risk that unauthorized persons could make changes to the system configuration or carry out acts of sabotage that could lead to power outages. For example, during critical operations such as switching transmission

lines or starting emergency generators, certainty about the operator's identity is crucial. The algorithm also enables quick verification of operators' identities during emergencies. This allows operators to react immediately to failures or cyberattacks, minimizing the risk of long-term power outages. For example, if unauthorized access or system manipulation is detected, biometric authentication allows access to be immediately blocked and authorized personnel to take control.

Biometric authentication mechanisms reduce the risk of insider attacks that may have access to systems. Even if an employee with malicious intent gains physical access to energy transmission management systems, they will not be able to carry out malicious activities without the appropriate biometric credentials.

The "Bio Command Authenticator" algorithm enables accurate tracking and auditing of operators' activities in the system. Each operation performed by an employee is logged and can be assigned to a specific person thanks to unique biometric features. This approach allows one to quickly identify and respond to unusual or suspicious activity that may indicate attempts to disrupt one's system.

In order to illustrate the operation of the system, two examples of preventing power outages can be cited:

- Example 1: In the case of a ransomware attack on power transmission management systems, the "Bio Command Authenticator" algorithm enables quick and secure authentication of operators responsible for restoring the system to operation. This makes it possible to minimize response time and limit the effects of an attack.
- Example 2: When unauthorized access to the system is detected, the algorithm immediately blocks access and triggers emergency procedures, allowing authorized operators to quickly take control and prevent potential power outages.

Integrating biometrics with a command-line interface (CLI) to protect critical infrastructure presents numerous challenges that must be effectively addressed to ensure reliable and secure operation of systems:

1. **Hardware and software compatibility:** Biometric authentication systems require specialized hardware (e.g., fingerprint scanners, facial recognition cameras, and iris scanners) and appropriate software to process biometric data. Integrating these components into existing CLI systems can be complex and expensive. Introducing hardware and software compatibility standards and ensuring interoperability between different devices and systems can make integration much easier.
2. **Biometric data security and privacy:** Storing and processing biometric data carries the risk of leakage or unauthorized access, which can lead to serious privacy and security breaches, but implementing advanced biometric data encryption methods and decentralized data storage can significantly reduce the risk. Additionally, regular security audits and compliance with legal regulations such as GDPR are essential to protect user privacy.
3. **Reliability of biometric authentication systems:** Biometric authentication systems can sometimes fail, for example, in the case of physical damage to biometric devices or changes in the user's biometric characteristics (e.g., finger injuries, changes in facial appearance), and here, the introduction of alternative authentication mechanisms, such as multi-factor authentication (MFA) which combines biometrics with other authentication methods (e.g., hardware tokens, passwords), can increase system reliability. Regular updates and maintenance of biometric equipment are also crucial.
4. **Integration with existing procedures and systems:** Implementing biometrics into existing CLI systems requires proper integration with current security procedures and operating systems, which can be a challenge from a technical and organizational point of view. However, conducting a detailed pre-implementation analysis and planning for a phased implementation can facilitate integration. The support of IT security experts and testing the system under controlled conditions before full implementation is also recommended.

5. **Implementation costs and possible economic and social consequences:** The selection of tools and their functionalities should be dictated by the specific needs and limitations of the company and the project in the short and long term. Security is a process; therefore, it will generate costs from both CAPEX (procurement costs) and OPEX (operating cost) perspectives. It is important that the investment in safety minimizes risk as much as possible. When looking at the social and economic effects, V. Gupta's "6 ways to die" model and the INAM matrix are often used.

In order to ensure that the development of the solution complies with the applicable regulations, a detailed analysis was also carried out according to the following standards:

- ISO/IEC 27001:2013—Information Security Management Systems: This solution is designed in accordance with the requirements of ISO/IEC 27001:2013, which ensures appropriate risk management and data protection. An example is the implementation of advanced biometric data encryption mechanisms and conducting regular security audits. The energy transmission management system, integrated with biometric authentication, takes into account security policies and risk management procedures, which ensures compliance with the ISO/IEC 27001:2013 standard [52].
- The NIST Cybersecurity Framework, a framework developed by the National Institute of Standards and Technology (NIST), provides guidelines for managing and reducing cyber risk in organizations. The framework includes five key functions: identification, protection, detection, response, and recovery. Integrating the developed biometric authentication mechanisms into existing procedures compliant with the NIST framework allows for better identification, protection, detection, response, and recovery from cyber incidents. An example is the use of real-time monitoring systems that use machine learning algorithms to identify anomalies and potential threats.
- IEC 62351—Protection Standards for Control and Automation Systems in Power Generation is a series of standards developed by the International Electrotechnical Commission (IEC) that focuses on the protection of control and automation systems used in the energy sector. The built algorithm has been adapted to the requirements of IEC 62351, which ensures compliance with international safety standards for energy systems. An example is the implementation of security measures in communication between control systems, which protects against unauthorized access and manipulation. The use of biometric authentication mechanisms ensures that only authorized operators can make changes to control systems, increasing the security and reliability of the energy infrastructure.
- GDPR—General Data Protection Regulation: The GDPR is a European data protection regulation that imposes obligations on organizations to store, process, and protect personal data. Biometric systems are designed with GDPR requirements in mind, ensuring that biometric data and user privacy are adequately protected. An example is the use of advanced methods of anonymization and pseudonymization of biometric data, which minimizes the risk of privacy breaches.

9. Conclusions

This article presents an innovative approach to managing the security of IT systems through the integration of the command-line interface (CLI) with biometrics. The proposed "BioCommand Authenticator" algorithm adds an extra layer of security by combining the precision and control offered by the CLI with users' unique biometric characteristics. This approach not only increases the level of security, but also simplifies the authentication process, which is particularly important in the context of critical energy infrastructure protection [53–58].

Critical energy infrastructure, including energy transmission management systems, is particularly vulnerable to cyberattacks due to its strategic importance and dependence on advanced IT systems. The integration of biometrics with cryptographic mechanisms provides a high level of protection against unauthorized access, while minimizing the risks associated with traditional authentication methods such as passwords. By using biometric

features, systems become less vulnerable to attacks, which significantly improves their reliability and resilience to cyber threats.

The application of this approach in the energy sector can significantly increase the stability and security of energy transmission management systems. By providing better protection against cyber threats, it is possible to minimize the risk of power outages, which could have catastrophic consequences for the economy and society [59–62].

In the future, further development and improvement in this type of solutions can contribute to even greater protection of critical infrastructure against growing threats. It will also be crucial to ensure that the solutions put in place comply with data protection regulations and meet high ethical standards in order to build trust in biometric technologies in security systems.

The proposed biometric-based approach offers significant advantages over traditional authentication methods such as passwords, both in terms of security and usability. Biometric features such as fingerprints, faces, and irises are unique to each individual user and extremely difficult to counterfeit. This provides a higher level of security, as an unauthorized user cannot easily copy or falsify biometric data. Passwords, on the other hand, are vulnerable to a variety of attacks, such as phishing, brute force, and social engineering. They can be easily guessed, stolen, or overheard, which poses a serious threat to system security.

In addition, users do not have to remember any complicated combinations or phrases, which eliminates the risk of forgetting passwords and using easy-to-guess passwords. The biometric authentication process is typically quick and intuitive. The user can simply place their finger on the scanner or look at the camera, which significantly increases the convenience of use.

For biometric authentication technologies to protect critical infrastructure even more effectively, further research and development is needed in several key areas. First of all, more advanced biometric data processing algorithms should be developed, which will be able to better recognize and analyze biometric features, even in difficult conditions (e.g., variable lighting and physical changes in users). Another aspect is to focus on lowering false-rejection rates (FRR) and false-acceptance rates (FAR) by improving pattern recognition techniques and introducing more advanced machine learning methods. Introducing more advanced methods of encrypting biometric data protects users from theft or unauthorized access. Techniques such as homomorphic encryption can make it possible to process encrypted data without the need to decrypt them and to implement decentralized methods of storing biometric data, such as blockchain, which can provide an additional level of security and resistance to attacks.

Author Contributions: Conceptualization, A.M. and M.B.; methodology, A.M. and M.B.; software, A.M., M.B., and M.W.H.; validation, A.M., A.B., and K.T.-O.; formal analysis, A.M., A.B., and K.T.-O.; investigation, A.M., A.B., and K.T.-O.; resources, A.B.; data curation, K.T.-O.; writing—original draft preparation, A.M., M.B., M.W.H., A.B., and K.T.-O.; writing—review and editing, A.M., M.B., M.W.H., A.B., and K.T.-O.; visualization, A.M., M.B., M.W.H., A.B., and K.T.-O.; supervision, A.M. and M.B.; project administration, A.M. and M.B.; funding acquisition, A.M. and M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Statutory Research BK-271/RG1/2024 and as part of the Excellence Initiative—Research University program of the Silesian University of Technology.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. She, R.; Liu, S.; Wan, S.; Xiong, K.; Fan, P. Importance of Small Probability Events in Big Data: Information Measures, Applications, and Challenges. *IEEE Access* **2019**, *7*, 100363–100382. [CrossRef]
2. Yu, J.-Y.; Lee, E.; Oh, S.-R.; Seo, Y.-D.; Kim, Y.-G. A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security. *IEEE Access* **2020**, *8*, 45304–45324. [CrossRef]
3. Son, J.; Choi, J.; Yoon, H. New Complementary Points of Cyber Security Schemes for Critical Digital Assets at Nuclear Power Plants. *IEEE Access* **2019**, *7*, 78379–78390. [CrossRef]
4. Aljohani, M.; Ahmad, I.; Basher, M.; Allassafi, M.O. Performance Analysis of Cryptographic Pseudorandom Number Generators. *IEEE Access* **2019**, *7*, 39794–39805. [CrossRef]
5. Ahmad, M.; Al-Solami, E.; Alghamdi, A.M.; Yousaf, M.A. Bijective S-Boxes Method Using Improved Chaotic Map-Based Heuristic Search and Algebraic Group Structures. *IEEE Access* **2020**, *8*, 110397–110411. [CrossRef]
6. Zahid, A.H.; Al-Solami, E.; Ahmad, M. A Novel Modular Approach Based Substitution-Box Design for Image Encryption. *IEEE Access* **2020**, *8*, 150326–150340. [CrossRef]
7. Özkaynak, F. Brief Review on Application of Nonlinear Dynamics in Image Encryption. *Nonlinear Dyn.* **2018**, *92*, 305–313. [CrossRef]
8. Radanliev, P. Cyber-attacks on Public Key Cryptography. *Preprints* **2023**, 2023091769. [CrossRef]
9. Ansaria, A. Analysis of Ukraine power grid cyber-attack 2015. *World J. Adv. Eng. Technol. Sci.* **2024**, *11*, 410–412. [CrossRef]
10. Khan, F.B.; Asad, A.; Durad, H.; Mohsin, S.M.; Kazmi, S.N. Dragonfly cyber threats: A case study of malware attacks targeting power grids. *J. Comput. Biomed. Inform.* **2023**, *4*, 172–185.
11. Available online: <https://www.skyboxsecurity.com/> (accessed on 9 July 2024).
12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union. Available online: <https://eur-lex.europa.eu/eli/dir/2022/2555> (accessed on 9 July 2024).
13. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (accessed on 16 July 2024).
14. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2557> (accessed on 10 July 2024).
15. Zhang, G.; Ding, W.; Li, L. Image Encryption Algorithm Based on Tent Delay-Sine Cascade with Logistic Map. *Symmetry* **2020**, *12*, 355. [CrossRef]
16. Kang, Y.; Huang, L.; He, Y.; Xiong, X.; Cai, S.; Zhang, H. On a Symmetric Image Encryption Algorithm Based on the Peculiarity of Plaintext DNA Coding. *Symmetry* **2020**, *12*, 1393. [CrossRef]
17. Thoai, V.P.; Kahkeshi, M.S.; Huynh, V.V.; Ouannas, A.; Pham, V.-T. A Nonlinear Five-Term System: Symmetry, Chaos, and Prediction. *Symmetry* **2020**, *12*, 865. [CrossRef]
18. Li, Z.; Peng, C.; Tan, W.; Li, L. A Novel Chaos-Based Color Image Encryption Scheme Using Bit-Level Permutation. *Symmetry* **2020**, *12*, 1497. [CrossRef]
19. Zhang, R.; Yu, L.; Jiang, D.; Ding, W.; Song, J.; He, K.; Ding, Q. A Novel Plaintext-Related Color Image Encryption Scheme Based on Cellular Neural Network and Chen's Chaotic System. *Symmetry* **2021**, *13*, 393. [CrossRef]
20. Muhammad, Z.M.Z.; Özkaynak, F. Security Problems of Chaotic Image Encryption Algorithms Based on Cryptanalysis Driven Design Technique. *IEEE Access* **2019**, *7*, 99945–99953. [CrossRef]
21. Singh, T.D.; Khilji, A.F.U.R.; Divyansha; Singh, A.V.; Thokchom, S.; Bandyopadhyay, S. Predictive Approaches for the UNIX Command Line: Curating and Exploiting Domain Knowledge in Semantics Deficit Data. *Multimed. Tools Appl.* **2021**, *80*, 9209–9229. [CrossRef]
22. Armstrong, M.E.; Jones, K.S.; Namin, A.S.; Newton, D.C. Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals. *ACM Trans. Comput. Educ.* **2020**, *20*, 1–25. [CrossRef]
23. Anand, D.; Kumar, A. IoT-Based Automated Healthcare System. In *Advanced Healthcare Systems*; Tanwar, R., Balamurugan, S., Saini, R.K., Bharti, V., Chithaluru, P., Eds.; Wiley: Hoboken, NJ, USA, 2022; pp. 335–350. ISBN 978-1-119-76886-9.
24. Kumar, K.S.; Srivatsan, M.; Kumar, S.S.; Satyaa, S.; Vishwamalyan, J.S. Passive RFID Encryption and Decryption Using CLI. In *Proceedings of the 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Kirtipur, Nepal, 11–13 October 2023; pp. 150–153.
25. Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Valli, C. Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry* **2019**, *11*, 141. [CrossRef]
26. Yang, W.; Wang, S.; Sahri, N.M.; Karie, N.M.; Ahmed, M.; Valli, C. Biometrics for Internet-of-Things Security: A Review. *Sensors* **2021**, *21*, 6163. [CrossRef]
27. Yang, W.; Wang, S.; Cui, H.; Tang, Z.; Li, Y. A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. *Sensors* **2023**, *23*, 3566. [CrossRef] [PubMed]
28. Yang, W.; Wang, S.; Shahzad, M.; Zhou, W. A Cancelable Biometric Authentication System Based on Feature-Adaptive Random Projection. *J. Inf. Secur. Appl.* **2021**, *58*, 102704. [CrossRef]

29. Dai, T.; Karve, A.; Koper, G.; Zeng, S. Automatically Detecting Risky Scripts in Infrastructure Code. In Proceedings of the 11th ACM Symposium on Cloud Computing, Virtual Event, 12 October 2020; pp. 358–371.
30. Abdelrahman, A.M.; Rodrigues, J.J.P.C.; Mahmoud, M.M.E.; Saleem, K.; Das, A.K.; Korotaev, V.; Kozlov, S.A. Software-defined Networking Security for Private Data Center Networks and Clouds: Vulnerabilities, Attacks, Countermeasures, and Solutions. *Int. J. Commun.* **2021**, *34*, e4706. [\[CrossRef\]](#)
31. Yang, X.; Yuan, J.; Yang, H.; Kong, Y.; Zhang, H.; Zhao, J. A Highly Interactive Honeypot-Based Approach to Network Threat Management. *Future Internet* **2023**, *15*, 127. [\[CrossRef\]](#)
32. Singh, A.S.B.; Yusof, Y.; Nathan, Y. EAGLE: GUI-Based Penetration Testing Tool for Scanning and Enumeration. In Proceedings of the 2021 14th International Conference on Developments in eSystems Engineering (DeSE), Sharjah, United Arab Emirates, 7–10 December 2021; pp. 97–101.
33. Clim, A.; Toma, A.; Zota, R.D.; Constantinescu, R. The Need for Cybersecurity in Industrial Revolution and Smart Cities. *Sensors* **2022**, *23*, 120. [\[CrossRef\]](#) [\[PubMed\]](#)
34. Mishra, A.; Alzoubi, Y.I.; Gill, A.Q.; Anwar, M.J. Cybersecurity Enterprises Policies: A Comparative Study. *Sensors* **2022**, *22*, 538. [\[CrossRef\]](#) [\[PubMed\]](#)
35. Tissir, N.; El Kafhali, S.; Aboutabit, N. Cybersecurity Management in Cloud Computing: Semantic Literature Review and Conceptual Framework Proposal. *J. Reliab. Intell. Environ.* **2021**, *7*, 69–84. [\[CrossRef\]](#)
36. Senol, M.; Karacuha, E. Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *J. Eng.* **2020**, *2020*, 5267564. [\[CrossRef\]](#)
37. Haddad, C.; Binder, C. Governing through Cybersecurity: National Policy Strategies, Globalized (in-) Security and Sociotechnical Visions of the Digital Society. *Osterr. Z. Soziologie* **2019**, *44*, 115–134. [\[CrossRef\]](#)
38. Paananen, H.; Lapke, M.; Siponen, M. State of the Art in Information Security Policy Development. *Comput. Secur.* **2020**, *88*, 101608. [\[CrossRef\]](#)
39. Weiss, M.; Biermann, F. Cyberspace and the Protection of Critical National Infrastructure. *J. Econ. Policy Reform* **2023**, *26*, 250–267. [\[CrossRef\]](#)
40. Tico, M.; Kuosmanen, P. Fingerprint Matching Using an Orientation-Based Minutia Descriptor. *IEEE Trans. Pattern Anal. Mach. Intell.* **2003**, *25*, 1009–1014. [\[CrossRef\]](#)
41. Wang, X.; Xue, H.; Liu, X.; Pei, Q. A Privacy-Preserving Edge Computation-Based Face Verification System for User Authentication. *IEEE Access* **2019**, *7*, 14186–14197. [\[CrossRef\]](#)
42. Oktiana, M.; Horiuchi, T.; Hirai, K.; Saddami, K.; Arnia, F.; Away, Y.; Munadi, K. Cross-Spectral Iris Recognition Using Phase-Based Matching and Homomorphic Filtering. *Heliyon* **2020**, *6*. [\[CrossRef\]](#) [\[PubMed\]](#)
43. Zhang, X.; Jing, K.; Song, G. Research and Development of Palmprint Authentication System Based on Android Smartphones. *Mob. Inf. Syst.* **2020**, *2020*, 8846192. [\[CrossRef\]](#)
44. Hammad, M.; Zhang, S.; Wang, K. A novel two-dimensional ECG feature extraction and classification algorithm based on convolution neural network for human authentication. *Future Gener. Comput. Syst.* **2019**, *101*, 180–196. [\[CrossRef\]](#)
45. Hammad, M.; Plawiak, P.; Wang, K.; Acharya, U.R. ResNet-Attention Model for Human Authentication Using ECG Signals. *Expert Syst.* **2021**, *38*, e12547. [\[CrossRef\]](#)
46. Nivedetha, B.; Vennila, I. FFBKS: Fuzzy Fingerprint Biometric Key Based Security Schema for Wireless Sensor Networks. *Commun.* **2020**, *150*, 94–102. [\[CrossRef\]](#)
47. Belguechi, R.; Cherrier, E.; Rosenberger, C.; Ait-Aoudia, S. Operational Bio-hash to Preserve Privacy of Fingerprint Minutiae Templates. *IET Biom.* **2013**, *2*, 76–84. [\[CrossRef\]](#)
48. Jin, A.T.B.; Ling, D.N.C.; Goh, A. Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number. *Pattern Recognit.* **2004**, *37*, 2245–2255. [\[CrossRef\]](#)
49. Luo, W.; Hu, Y.; Jiang, H.; Wang, J. Authentication by Encrypted Negative Password. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 114–128. [\[CrossRef\]](#)
50. Hu, S.; Li, M.; Wang, Q.; Chow, S.S.; Du, M. Outsourced biometric identification with privacy. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2448–2463. [\[CrossRef\]](#)
51. Barni, M.; Bianchi, T.; Catalano, D.; Di Raimondo, M.; Labati, R.D.; Failla, P.; Fiore, D.; Lazzeretti, R.; Piuri, V.; Piva, A.; et al. A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercodes Templates. In Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010; pp. 1–7.
52. ISO/IEC 27001:2023-08; International Standard Standardizing Information Security Management Systems. ISO: Geneva, Switzerland, 2023.
53. Cybercriminals Attack Users with 400,000 New Malicious Files Daily—That Is 5% More Than in 2021. Available online: https://www.kaspersky.com/about/press-releases/2022_cybercriminals-attack-users-with-400000-new-malicious-files-daily--that-is-5-more-than-in-2021 (accessed on 4 June 2024).
54. Microsoft Mitigated Record-Breaking 3.47 Tbps DDoS Attack on Azure Customers. Available online: <https://thehackernews.com/2022/01/microsoft-mitigated-record-breaking-347.html> (accessed on 4 June 2024).
55. Hao, Z.; Feng, Y.; Koide, H.; Sakurai, K. A Sequential Detection Method for Intrusion Detection System Based on Artificial Neural Networks. *Int. J. Netw. Comput.* **2020**, *10*, 213–226. [\[CrossRef\]](#) [\[PubMed\]](#)

56. Morgan, S. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. *Cybercrime Magazine*, 13 November 2018.
57. Lyu, Y.; Feng, Y.; Sakurai, K. A Survey on Feature Selection Techniques Based on Filtering Methods for Cyber Attack Detection. *Information* **2023**, *14*, 191. [[CrossRef](#)]
58. Chen, C.-M.; Chen, Y.-L.; Lin, H.-C. An Efficient Network Intrusion Detection. *Comput. Commun.* **2010**, *4*, 477–484. [[CrossRef](#)]
59. Shams, E.A.; Rizaner, A. A Novel Support Vector Machine Based Intrusion Detection System for Mobile Ad Hoc Networks. *Wirel. Netw.* **2018**, *24*, 1821–1829. [[CrossRef](#)]
60. Stein, G.; Chen, B.; Wu, A.S.; Hua, K.A. Decision Tree Classifier for Network Intrusion Detection with GA-Based Feature Selection. In Proceedings of the 43rd Annual Southeast Regional Conference, Kennesaw, Georgia, 18 March 2005; Volume 2, pp. 136–141.
61. Farnaaz, N.; Jabbar, M.A. Random Forest Modeling for Network Intrusion Detection System. *Procedia Comput. Sci.* **2016**, *89*, 213–217. [[CrossRef](#)]
62. Ashiku, L.; Dagli, C. Network Intrusion Detection System Using Deep Learning. *Procedia Comput. Sci.* **2021**, *185*, 239–247. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.