Journal of Science and Technology
ISSN: 2456-5660 Volume 9, Issue 1 (JAN -2024)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2024.v9.i1.pp21-29*

A Fernet Based Lightweight Cryptography Adopted Enhancing Certificate Validation through Blockchain Technology

K. Obulesh[1], R. Laxmi Prasana[2], S. Lakshmi Supraja[2], Sameena Begum[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science Engineering
[1,2]Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Kompally,
Secunderabad-500100, Telangana, India

To Cite this Article

K. Obulesh, R. Laxmi Prasana, S. Lakshmi Supraja, Sameena Begum**, "A Fernet Based Lightweight Cryptography Adopted Enhancing Certificate Validation through Blockchain Technology"** *Journal of Science and Technology, Vol. 09, Issue 01 - JAN 2024, pp21-29*

Article Info

Received: 25-12-2023 Revised: 05 -01-2024 Accepted: 15-01-2024 Published: 25-01-2024

ABSTRACT

Certificate forgery has become a pervasive issue, necessitating a transformative approach to validation processes. The limitations of traditional methods have prompted the exploration of cutting-edge technologies, with blockchain emerging as a promising solution. The conventional system relies on manual verification processes that are time-consuming, opaque, and prone to fraudulent activities. Physical examination of paper-based certificates and reliance on centralized databases make the system vulnerable to tampering and counterfeiting. The drawbacks of the current system include its susceptibility to data manipulation, lack of transparency, and inefficiency. This section critically evaluates the shortcomings of traditional certificate validation methods, setting the stage for the proposed blockchain-based solution.The proposed system leverages blockchain technology, specifically implementing the Fernet Based Lightweight Cryptography (Fernet-LWC) algorithm, to enhance the security and efficiency of certificate validation. The Fernet-LWC algorithm offers cryptographic protection, ensuring the integrity and confidentiality of certificate data. The blockchain's decentralized nature eliminates the need for a central authority, reducing the risk of data manipulation and fostering trust in the validation process. Each certificate issuance is securely recorded on the blockchain, creating an immutable and transparent trail. This section delves into the technical aspects of the proposed system, providing a detailed explanation of how the Fernet-LWC algorithm ensures data security and integrity. A comprehensive analysis of the proposed system's architecture and implementation details is presented. This includes the integration of the Fernet-LWC algorithm into the blockchain framework, ensuring a secure and efficient certificate validation process. The system's components, their interactions, and the underlying cryptographic mechanisms are elucidated, providing a clear understanding of how the proposed solution operates.

Keywords: Block Chain Technology, adopted enhancing, lighgt weight cryptography, fernet.

1. INTRODUCTION

A blockchain-based secure and efficient validation system for digital certificates represents a groundbreaking solution to address the challenges associated with certificate verification, authentication, and fraud prevention. This system leverages the inherent characteristics of blockchain technology, such as immutability, transparency, and decentralization, to revolutionize the way digital certificates are managed and verified.

At its core, this system operates by storing digital certificate data on a blockchain ledger, ensuring that once a certificate is issued, it cannot be tampered with or altered. Each certificate is represented as a unique digital token on the blockchain, making it easy to verify its authenticity and origin. Furthermore, the decentralized nature of blockchain ensures that there is no single point of failure, reducing the risk of data breaches and unauthorized access.

Efficiency is a key feature of this system. Traditional methods of certificate validation can be time-consuming and susceptible to errors. With blockchain, verification becomes instantaneous and highly reliable. Institutions, employers, and individuals can quickly confirm the legitimacy of a certificate by accessing the blockchain, eliminating the need for time-consuming manual checks.

Security is paramount in this system. The cryptographic nature of blockchain technology ensures that data is encrypted and protected against unauthorized access. This safeguards sensitive certificate information from potential hackers and fraudulent activity. Moreover, the transparency of blockchain allows stakeholders to track the entire history of a certificate, from issuance to validation, enhancing trust and accountability.

Additionally, this system promotes interoperability and reduces reliance on central authorities. Certificates from various sources and institutions can coexist on the same blockchain, facilitating cross-validation and making it easier for individuals to showcase their qualifications and achievements across different platforms and industries.

So, a blockchain-based secure and efficient validation system for digital certificates represents a paradigm shift in the way we manage and authenticate credentials. By harnessing the power of blockchain, this system offers a robust, tamper-proof, and transparent solution that enhances security, efficiency, and trust in the digital certificate ecosystem. It has the potential to streamline verification processes, reduce fraud, and empower individuals to take control of their digital identities and qualifications.

2. LITERATURE SURVEY

The proliferation of industrial IoT applications and networking services has facilitated a tremendous increase in the number of connected devices. These application devices can capture real-time industrial data with a dedicated sensor unit [1]. Industrial advancement and technological guidance are behind this shift in how systems interact with physical and logical things. A centralized architecture is used to communicate real-time industrial data and evaluate the critical components of IoT, including identity management [2]. A single failure point is feasible due to this common technique [3]. A significant issue with the Internet of Things (IoT) is the difficulty in maintaining and managing many connected devices [4]. A system of networks can talk interactively through adaptive self-configuration. IoT applications can be commercialized over the 6G network. A fundamental component of the IoT, the wireless sensor network (WSN) gathers and transmits physical data using various heterogeneous models [5].

Data security is a major concern of IoT systems because they are built by connecting many IoT devices [6]. Data generated by these devices are stored in the cloud and transmitted across various networks. A cyber-attack on a smart healthcare system can substantially impact the system's ability to produce and supply electricity. In addition to financial and other types of damage, cyber-attacks on smart healthcare can cause operational failures, power outages, the theft of critical data, and complete security breaches [7]. Cyber experts face difficulties keeping tabs on everything that passes via a smart grid and recognizing potential threats and attacks. Even though machine learning has become an essential part of cybersecurity, the problem is that this field requires distinct approaches and theoretical viewpoints to handle the enormous volume of data generated and transported across numerous networks in a smart grid [8]. The attacks and threats that could be launched against this proof-of-concept environment are being determined using threat modeling. Several potential threats have been tested, including detection, tampering, repudiation, information leakage, denial of service (DoS), and extended privilege (EoP). Each of the risks and the security elements associated with them are addressed using STRIDE. STRIDE is a typical threat modeling technique for finding and classifying attack vectors [9]. Using the well-known industrial framework MITRE ATTCK, researchers can detect threats disguised as tactics, techniques, and procedures (TTP) [10].

Based on the above, blockchain technology could be one of the main solutions for IoT security issues [11]. A blockchain provides a decentralized system using a consensus mechanism and smart contracts [12].

3. PROPOSED SYSTEM

Overview

Figure 4.1 shows the proposed system model. The detailed operation illustrated as follows:

Step 1. Input Certificates: This likely represents the starting point of the research. Input certificates refer to the digital certificates that need to be validated or verified. These certificates could be various types such as educational diplomas, professional certifications, or any other forms of digital credentials.

Step 2. Certificate Issuance and Verification System: This component suggests the existence of a system responsible for issuing and verifying digital certificates. In the context of the research, it's important to examine how this system currently works and identify its strengths and weaknesses.

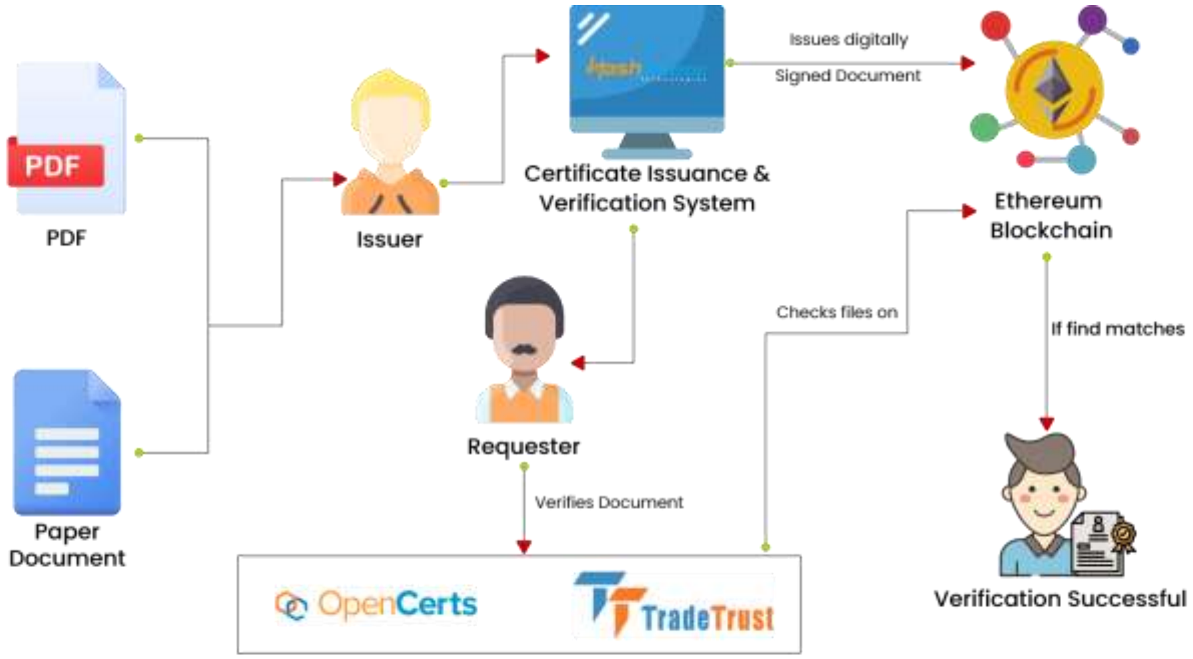


Figure.1: Proposed System model.

Step 3. Ethereum (Blockchain): Ethereum is mentioned as the blockchain technology that is likely being proposed or utilized in the research. Ethereum is a popular platform for developing blockchain-based applications. In this research, it's important to explain how Ethereum is used to enhance the security and efficiency of the certificate validation process.

Step 4. Requester: The "requester" is likely a user or entity that initiates the certificate validation process. In a blockchain-based system, this could be someone who wants to verify the authenticity of a digital certificate.

Step 5. Verification Results: This component indicates the outcome of the certificate validation process. It's essential to understand how the blockchain-based system generates and communicates verification results, including whether a certificate is valid or not.

4.2 Ethereum

Ethereum is a decentralized blockchain platform that allows developers to build decentralized applications (dApps) and execute smart contracts. It was launched in 2015 by Vitalik Buterin and quickly became one of the most popular blockchain platforms in the world, second only to Bitcoin in terms of market capitalization.

Ethereum's main innovation is the ability to create smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. These smart contracts are executed on the Ethereum Virtual Machine (EVM), which is a decentralized, Turing-complete virtual machine that runs on the Ethereum network.

The Ethereum network also has its own cryptocurrency called Ether (ETH), which is used to pay for transaction fees and computational services on the network. ETH is also used as a store of value and traded on cryptocurrency exchanges.

Advantages of Ethereum

Ethereum provides several advantages over other blockchain platforms and traditional systems. Here are some of the main advantages of Ethereum:

Smart Contracts: Ethereum's main innovation is the ability to create smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. This allows for secure and automated execution of complex agreements without the need for intermediaries or third parties.

Decentralization: Ethereum is a decentralized platform, which means that it is not controlled by any single entity or organization. This provides a level of trust and transparency, as there is no single point of failure or vulnerability.

Interoperability: Ethereum's blockchain is open-source and allows for interoperability with other blockchain platforms, making it easier to integrate with existing systems and applications.

Programmable: Ethereum's blockchain is programmable, which means that developers can create custom applications and smart contracts that meet their specific needs. This allows for more flexibility and customization than traditional systems.

Security: Ethereum's blockchain is secured through cryptographic algorithms and consensus mechanisms, making it resistant to hacking and fraud. Additionally, smart contracts on the platform are auditable and transparent, which helps to reduce the risk of fraud and corruption.

Tokenization: Ethereum enables the creation and exchange of tokens, which can represent assets, securities, or other digital assets. This makes it possible to create new business models and revenue streams that were previously not possible.

Overall, Ethereum provides a powerful and flexible platform for developers to build decentralized applications and execute complex smart contracts in a secure, transparent, and decentralized manner.

Blockchain

Blockchain is a decentralized, digital ledger technology that is used to record and store data in a secure and transparent manner. It is a distributed ledger, meaning that it is maintained by a network of computers, rather than being controlled by a single entity. Each block in the chain contains a set of transactions, and once a block is added to the chain, it cannot be altered or deleted. This makes blockchain an immutable and tamper-resistant technology that is particularly well-suited for storing and transmitting sensitive data.

Blockchain technology is perhaps best known for its use in cryptocurrencies like Bitcoin and Ethereum, but it has a wide range of other potential applications as well. These include supply chain management, identity verification, voting systems, and more. The decentralized nature of blockchain means that it has the potential to disrupt a variety of industries and business models by enabling trust and transparency in transactions and data exchange.

4. RESULTS AND DISCUSSION

Results description

Figure 2 shows the initial state of the graphical user interface (GUI) when the application is launched. It includes the following elements:

- Title: "PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION"
- Buttons: "Store Certificate in Blockchain" and "Certificate Verification"
- Entry fields for student details (Roll Number, Student Name, Contact Information)
- A text widget for displaying information and results.
- The main window with a specific size and background color (powder blue)

Figure 3 represents the GUI after a user has filled in the student's details. It includes the following changes from Figure 2:

- The entry fields for Roll Number, Student Name, and Contact Information are populated with user input.
- The user has entered the relevant information required for storing a certificate in the blockchain.

Figure 4 shows the GUI after the user has clicked the "Store Certificate in Blockchain" button and the certificate has been successfully stored in the blockchain. It includes the following changes:

- Information about the stored certificate, such as its digital signature and blockchain details, is displayed in the text widget.

— The user receives confirmation that the certificate has been successfully added to the blockchain.

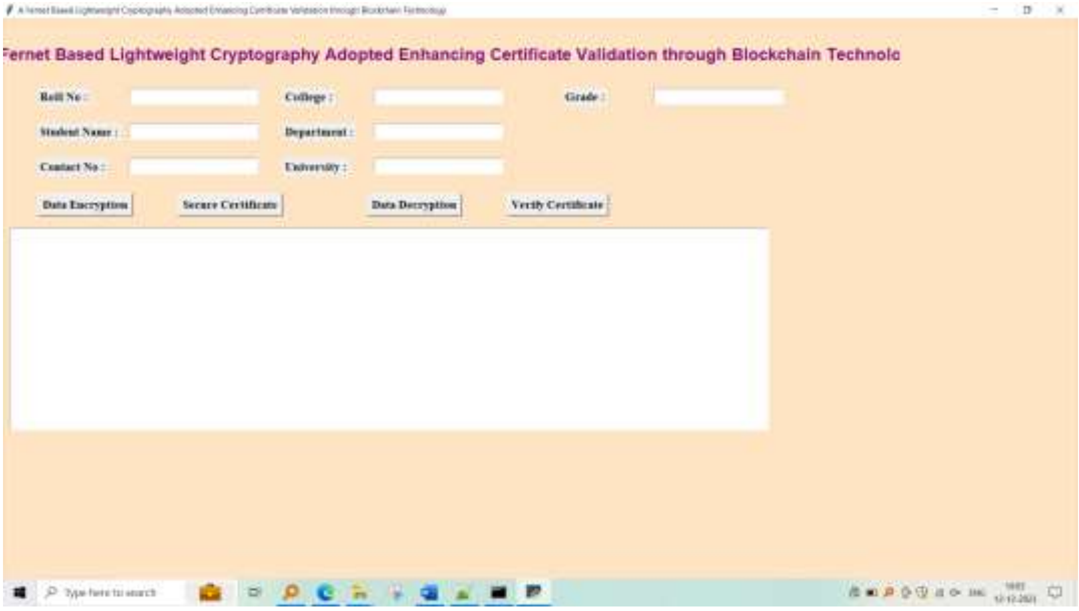
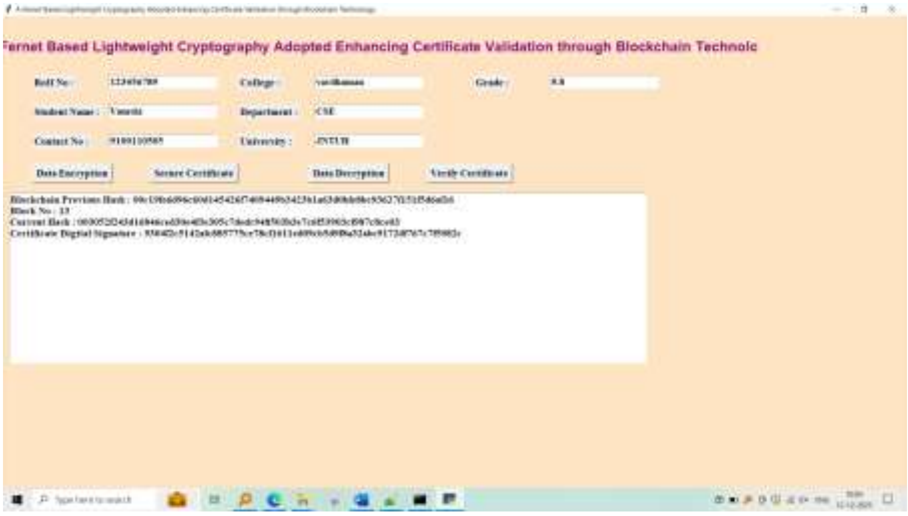


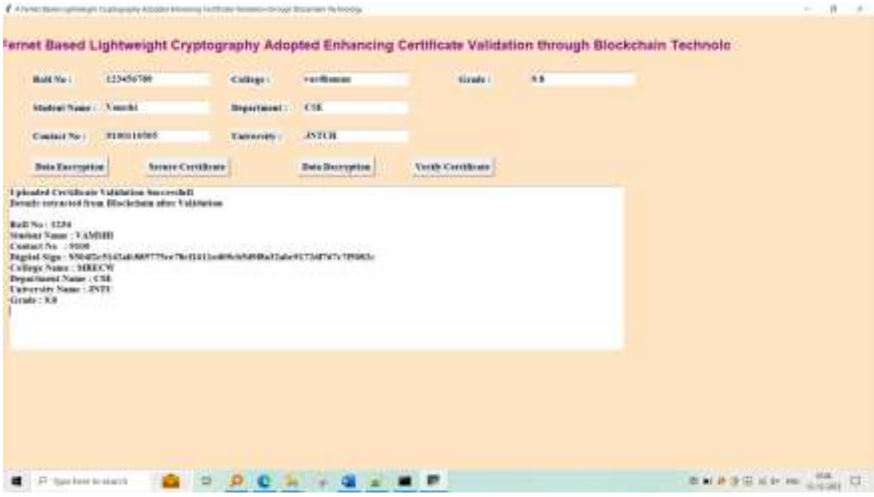
Figure 2: Main GUI application of proposed blockchain powered certificate verification for forgery prevention.


Fernet Based Lightweight Cryptography Adopted Enhancing Certificate Validation through Blockchain Technolo
Data Encryption
Secure Certificate
Data Decryption
Verify Certificate
Type here to search

Roll No : 123456789
College : vardhaman
Grade : 8.8
Student Name : Vasrithi
Department : CSE
Contact No : 9100110585
University : JNTUH

Blockchain Previous Hash : [illegible]
Block No : 13
Current Hash : [illegible]
Certificate Digital Signature : [illegible]

Figure 3: GUI application after entering the details of student with roll number, student name, and contact information.

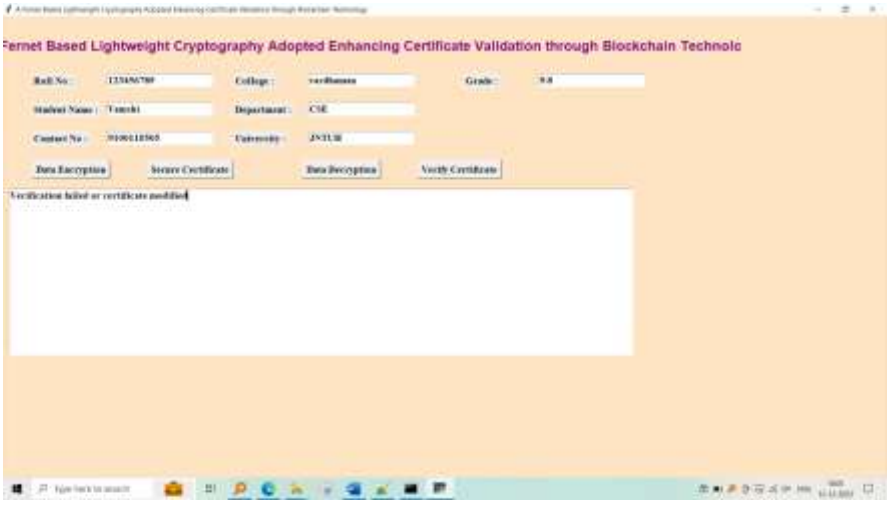

Fernet Based Lightweight Cryptography Adopted Enhancing Certificate Validation through Blockchain Technolo
Data Encryption
Secure Certificate
Data Decryption
Verify Certificate

Roll No :	123456789	College :	vardhaman	Grade :	9.8
Student Name :	Vamshi	Department :	CSE		
Contact No :	9100110505	University :	JNTUH		

```
Uploaded Certificate Validation Successfull
Details extracted from Blockchain after Validation

Roll No : 1234
Student Name : VAMSHI
Contact No : 9000
Digital Sign : [illegible]
College Name : MRECW
Department Name : CSE
University Name : JNTU
Grade : 9.8
```

Figure 4: Illustration of proposed GUI application after storing the certificate with student entry details.


Fernet Based Lightweight Cryptography Adopted Enhancing Certificate Validation through Blockchain Technolo
Data Encryption
Secure Certificate
Data Decryption
Verify Certificate

Roll No :	123456789	College :	vardhaman	Grade :	9.8
Student Name :	Vamshi	Department :	CSE		
Contact No :	9100110505	University :	JNTUH		

```
Verification failed or certificate modified
```

Figure 5: Checking the certificate verification with test template as input and displaying the validation is successfully verified with student enrolment.

In Figure 5, the user appears to be using the application to verify a certificate's authenticity that includes the following elements:

- The user has clicked the "Certificate Verification" button.
- A file dialog or input field is displayed for the user to select a test template (likely a certificate template) for verification.
- After selecting the template, the application calculates its digital signature and compares it to the blockchain's records.
- The text widget displays a message indicating successful verification, along with student enrolment details.

Figure 5 shows the GUI when the certificate verification process has failed or when the certificate has been modified. It includes the following elements:

- The user has attempted to verify a certificate, but the digital signature does not match any records in the blockchain.
- The text widget displays a message indicating that the verification has failed or that the certificate has been tampered with.

5. Conclusion And Future Scope

In conclusion, the implementation of blockchain technology in certificate verification holds immense potential for combating the persistent problem of certificate forgery across various industries. By offering a decentralized, tamper-resistant, and transparent platform, this innovative approach addresses the limitations of traditional verification methods. The immutability of blockchain ensures that certificate records remain secure and unalterable, thereby enhancing their credibility and authenticity. Additionally, the elimination of central authorities reduces the risk of data manipulation and fosters trust in the verification process. However, to fully realize the benefits of blockchain-powered certificate verification, several challenges must be overcome. These include ensuring widespread adoption of the technology, addressing scalability issues, and developing user-friendly interfaces for individuals and institutions.

REFERENCES

[1]. Siam, A.I.; Almaiah, M.A.; Al-Zahrani, A.; Elazm, A.A.; El Banby, G.M.; El-Shafai, W.; El-Samie, F.E.A.; El-Bahnasawy, N.A. Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. Comput. Intell. Neurosci. 2021, 2021, 8016525.

[2]. Ali, A.; Pasha, M.F.; Fang, O.H.; Khan, R.; Almaiah, M.A.; KAl Hwaitat, A. Big data based smart blockchain for information retrieval in privacy-preserving healthcare system. In Big Data Intelligence for Smart Applications; Springer International Publishing: Cham, Switzerland, 2022; pp. 279–296. [Google Scholar]

[3]. Altulaihan, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. Electronics 2022, 11, 3330. [Google Scholar]

[4]. Hasnain, M.; Pasha, M.F.; Ghani, I.; Mehboob, B.; Imran, M.; Ali, A. Benchmark Dataset Selection of Web Services Technologies: A Factor Analysis; IEEE Access: Piscataway, NJ, USA, 2020; Volume 8, pp. 53649–53665. [Google Scholar]

[5]. Ali, A.; Rahim, H.A.; Pasha, M.F.; Dowsley, R.; Masud, M.; Ali, J.; Baz, M. Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. Electronics 2021, 10, 2034. [Google Scholar]

[6]. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. An AI-Enabled Hybrid Lightweight Authentication Model for Digital Healthcare Using Industrial Internet of Things Cyber-Physical Systems. Sensors 2022, 22, 1448. [Google Scholar]

[7]. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Srivastava, G.; Karimipour, H. Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks. Comput. Ind. 2023, 144, 103801.

[8]. Hameed, K.; Ali, A.; Naqvi, M.H.; Jabbar, M.; Junaid, M.; Haider, A. Resource management in operating systems-a survey of scheduling algorithms. In Proceedings of the International Conference on Innovative Computing (ICIC), Lanzhou, China, 2–5 August 2016; Volume 1. [Google Scholar]

[9]. Singh, H.; Ahmed, Z.; Khare, M.D.; Bhuvana, J. An IoT and Blockchain-Based Secure Medical Care Framework Using Deep Learning and Nature-Inspired Algorithms. Int. J. Intell. Syst. Appl. Eng. 2023, 11, 183–191. [Google Scholar]

[10]. Kim, H.; Kim, S.-H.; Hwang, J.Y.; Seo, C. Efficient Privacy-Preserving Machine Learning for Blockchain Network. IEEE Access 2019, 7, 136481–136495. [Google Scholar]

[11]. Sharma, P.; Namasudra, S.; Crespo, R.G.; Parra-Fuente, J.; Trivedi, M.C. EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. Inf. Sci. 2023, 629, 703–718. [Google Scholar]

[12]. Almadani, M.S.; Alotaibi, S.; Alsobhi, H.; Hussain, O.K.; Hussain, F.K. Blockchain-based multi-factor authentication: A systematic literature review. Internet Things 2023, 23, 100844.