Available online at: http://www.advancedscientificjournal.com
http://www.krishmapublication.com
IJMASRI, Vol. 1, issue 1, pp. 96 - 104, Apr. -2025
https://doi.org/10.53633/ijmasri

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY ADVANCED SCIENTIFIC RESEARCH AND INNOVATION (IJMASRI)

ISSN: 2582-9130 IBI IMPACTFACTOR 1.5 DOI: 10.53633/IJMASRI

RESEARCH ARTICLE

ENHANCED DATA SECURITY AND PRIVACY USING BLOCK CHAIN TECHNOLOGY AND HYBRID ENCRYPTION ALGORITHM

Ms Dhivya E[1] and Dr Narmatha V[2]
[1]*ResearchScholar, Department of Computer and Information Science, Annamalai University*
Email: dhivyahasina0510@gmail.com
[2]*Assistant Professor / Programmer, Department of Computer and Information Science, Annamalai University*
Email: balaji.narmatha8@gmail.com

Abstract

Strong data security is crucial in an era where digital technology is pervasive. Security concerns are a significant issue in the modern world. The majority of the system gives a high degree of security to assure a safe connection and protect sensitive information from alteration and third- party access. However, hackers continue to scale every technology in an attempt to hijack the authorized network. Block chain technology and encryption have been used in the research to prevent such a scenario. This research recommends combining the block chain and two authentication techniques to encrypt a portion of the system in order to offer high-security data. The first level of authentication would be hybrid encryption, which combines the face recognition technique with the Diffie - Hellman Key Exchange and Two fish algorithms to offer authorization and authentication. After system activation, data sharing will protect the owner or organization from unwanted access and increase the reliability of data stored utilizing the blockchain technology technique. The system would keep all of the data in an encrypted way. The files should be hidden from others and unviewable by disabling the system. These technologies offer increased security and defense against attacks for extremely sensitive data.

Keywords: Blockchain Technology, Hybrid Encryption Algorithm, Two Factor Authentication, Face Recognition.

Introduction

Security has been one of the most significant considerations in all technical sectors in recent years. Information security is the primary problem with the vital advancement of technology in accordance with human needs. The growing digitization of sensitive information provides a threat to traditional security

techniques. Hardware and software resources are necessary for the vast majority of technologies. The development of a gateway in any of today's technological requirements could allow hackers to gain access to these systems and obtain the necessary authorization. In many areas that resemble banking transfers, transactions involving sensitive information like Aadhar IDs, debit cards, and credit cards are carried out over a network. Also, in the era of big data digitization and greater global connectivity, protecting sensitive information is more crucial than ever. Our dependence on digital data is visible in everything from private conversations and business transactions to state secrets and medical records, and the risks associated with this dependence increase. If a network isn't secure or has a gateway, Intruders can easily get access to it and take away the data for their own gain. In another instance, the records of an organization include customer information, employee information, and the organization's wind, and information is shared between consumers and staff. Sometimes all of the data is saved on a server via the system. An attacker should have access to every system within a company if they are able to employ social engineering tactics to get at the server's tiny printing. Thus, the most significant concept in the digital era is data security.

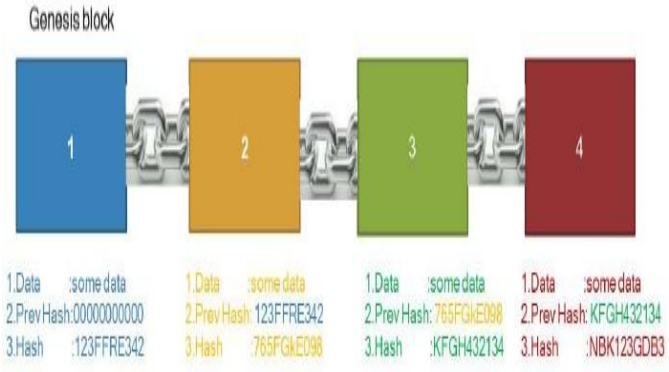
Due to the widespread use of computer networks worldwide, computer security also known as information security has emerged as the most significant global issue. The issue of how to protect the magical world from attack is crucial for engineers and directors, and their biggest task is to create entirely new methods that can detect attempts to compromise the network's efficiency and integrity. We refer to this area as the Intrusion Detection System (IDS). In the area of technology, there are absolutely more solutions than anticipated for making a replacement exceptional creation, which produces a better future. Each creation has also had some degree of significance, as technological advancements have made it easier and faster to reduce danger in addition to improving processes.

A. DOMAIN OVERVIEW

"A blockchain is an ever-expanding collection of records, or blocks, that are connected and protected by cryptography." Satoshi Nakamoto first proposed the idea in 2009.

BLOCK

1. Data:“HelloEveryone”
2. PrevHash:23432FRT123
3. 123FFRE342

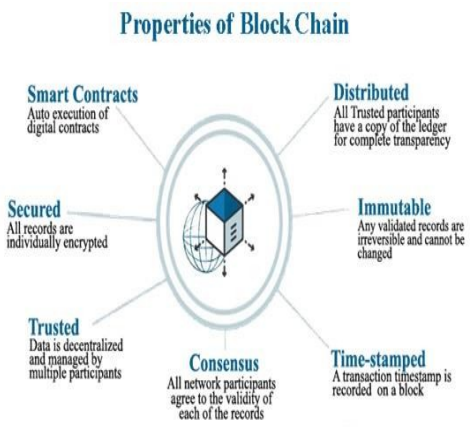


BLOCKCHAIN

Figure 1: Blockchain

Blockchain technology is a distributed ledger system that securely and impenetrably records transactions over a network of computers. The blockchain generates a chain of blocks that guarantees the integrity of the data by including a cryptographic hash of the preceding block in each block. Peer-to-peer transactions are made possible by this decentralized design, which does away with the need for middlemen like banks or clearing institutions.

In order to guarantee the security and integrity of data within the blockchain, cryptography is essential. It gives tools for creating digital signatures, encrypting data, and confirming the legitimacy of transactions. Blockchain would be open to several attacks without cryptography, including data manipulation and double- spending.



Understanding Blockchain Technology

Fundamentally, a blockchain is a decentralized record of every transaction that takes place within a network. Dispersed networks of computers, known as nodes, collaborate to validate and record transactions in this ledger.

Key features of blockchain technology include:

1. **Decentralization:** Blockchain is not dependent on a single central authority like conventional centralized databases are. Rather, a copy of the whole ledger is owned by every network participant, increasing transparency and lowering the possibility of data corruption.
2. **Immutability:** It is very hard to change data once it is stored on a blockchain. Cryptographic hashing and a consensus process that assures all nodes concur on the data's validity are used to achieve this immutability.
3. **Transparency:** Every participant in the network can see every transaction that is recorded on the blockchain. This openness can greatly lower fraud and improve user confidence.
4. **Security:** Blockchain uses modern cryptography methods to protect data. Because each block in the chain is connected to the one before it via a cryptographic hash, it is impervious to unwanted modifications.

B. OVERVIEW OF CRYPTOGRAPHY

The technique of using codes to secure communications and information so that only the intended recipients and ecipher and process it is known as cryptography. Consequently, information access is kept safe. The suffix "graphy" signifies "writing," while the prefix "crypt" means "hidden."

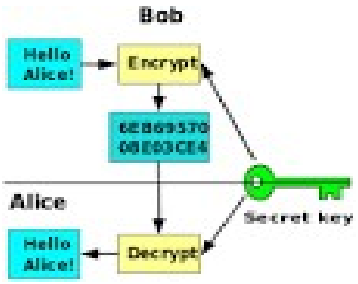


Figure2: Overview of Cryptography

There are five primary functions of cryptography:

1. ***Privacy/confidentiality:*** to make sure the designated recipient is the only person who can read the message.
2. ***Authentication:*** The act of authenticating one self.
3. ***Integrity:*** confirming to the recipient that there has been no change made to the original message.
4. ***Non - repudiation:*** away to verify that this message was actually sent by the sender.
5. ***Key exchange:*** the process via which sender and recipient exchange crypto keys.

Cryptography in Blockchain

Symmetric vs Asymmetric Cryptography

In compared to asymmetric cryptography, which uses a pair of keys - a public key and a private key - symmetric cryptography uses a single key for both data encryption and decryption. Asymmetric cryptography offers more security and permits safe communication between parties without requiring a shared secret key, whereas symmetric cryptography is quicker and more effective.

Hash Functions and Digital Signatures

A fixed-size output (hash value) that is specific to the input data is produced by mathematical methods known as hash functions from an input (or message).

Blockchain hash functions are one-way, which means that reversing the original input from the hash value is computationally impossible. Asymmetric cryptography is used to establish digital signatures, which give users a means to authenticate a message or transaction without disclosing their private key.

Public and Private Keys

Apair ofkeys - a public keyanda privatekey - are essential to public-key cryptography, sometimes referred to as asymmetric cryptography. While the private key is kept confidential and used for decryption or signature, the public key is freely shared and used for encryption or verification. Blockchain uses public and private keys to manage access to digital assets, create digital signatures, and authenticate transactions.

1.1 Objective

The primary objective of this paper is to have a high level of security so that a third party cannot enter the network without authorization. Several fields, including public services, business organization, and medical data, are supported by the use of blockchain technology and encryption. As technology improves, the motivation for security grows along with the scope of big data security.

1. LITERATURE SURVEY

This section reviews the short surveys of related works for the suggested algorithms and identifies the advantages and disadvantages of the current methods.

In 2024 Itisha Jain, "Blockchain Technology and Cryptography" This research paper explores the foundational principles of blockchain technology and cryptography, their interplay, and their applications across different sectors. Furthermore, to examine the challenges and opportunities posed by the integration of blockchain and cryptography and highlight potential future developments in this dynamic field [1].

In 2024 Chandan Kalita, Sikdar Md S. Askari, Mirzanur Rahman, Rabinder Kumar Prasad, Bikramjit Choudhury and Moirang them Tiken Singh, This paper introduces a "novel blockchain-based approach for secureand efficient databasemanagement". Blockchain technology, with its decentralized, immutable, and transparent nature, offers significant advantages over traditional database systems, particularly in enhancing data security, integrity, and audit ability. [2].

In 2023 Asma Mubark Alqahtani, Abdulmohsen Algarni "A Survey on Blockchain Technology Concepts, Applications and Security" This paper aims to provide an overview of blockchain technology and its security issues for users and researchers. This paper includes a comparison of consensus algorithms and a description of cryptography. Further, in this paper also analyzing real attacks and then summarizing security measures in blockchain [3].

In 2023 Sartaj Ahmad , Shubham Kumar Arya, Shobhit Gupta, Puneeta Singh and Sanjeev Kumar Dwivedi" Study of Cryptographic Techniques Adopted in Blockchain", In this paper, the main ideas of cryptography - such as encryption, hashing, digital signatures, and public-key cryptography - as well as their applications in blockchain technology are discussed. The significance of cryptography in the blockchain is examined in the paper, with a focus on protecting user data privacy, maintaining data integrity, and authenticating transactions [4].

1. PROPOSED METHOD

We have used the blockchain technology method and hybrid encryption method along with face recognition; encryption is used to the user's authorization related to level authentication while the face recognition is used to identify the authentication of the owner of the system. And the blockchain method is used to protect data sharing through the system harmfulness. Every piece of data is stored in an encrypted format. When the system is disabled, an outsider utilizing it is unable to determine what information was entered into the system. By combining these technologies, the system can benefit from complex security, authorization, confidentiality, and information integrity.

A hybrid encryption algorithm combines symmetric and asymmetric encryption to protect data. It's more secure than using just one method because it combines the strengths of both.

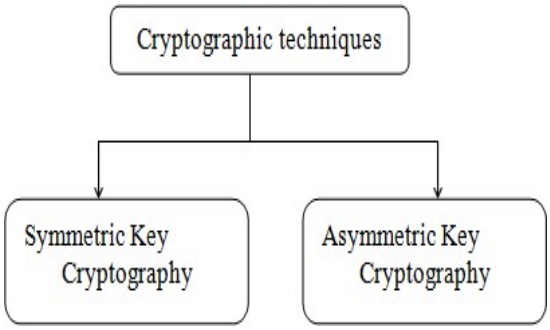


Figure3: Cryptography Techniques

In this Cryptography technique, we are using two methods. Namely,

- Diffie Hellman Key Exchange
- Two fish Algorithm

Difffie Hellman Key Exchange

A highly secure digital encryption technique called Diffie - Hellman key exchange allows two parties to exchange cryptographic keys over a public channel without their communication being sent over the internet.

Diffie – Hellman Key Exchange Algorithm steps:

Step 1: User A generates domain parameters p,q and g.

Step 2: UserAgeneratesarandomprivatekey XA.

Step 3: User A calculates public key as $Y_A=g^X$ Amod p.

Step 4: User A sends (p, g,Y_A) to user B.

Step 5: User B generates a random private key XB.

Step 6: User B calculates public key $Y_B = g^X$ Bmodp.

Step 7: User B calculates as

$K=(YA)^X$ Bmodp = $(g^XA)^X$ Bmodp=$g^{XA.XB}$ modp

Step 8: User Bsends Y_B to user A.

Step7: User A calculates as

$K=(YB)^X$Amodp= $(g^XB)^X$Amodp = $g^{XA.XB}$ modp

Two fish Algorithm

Two fish is a symmetric block cipher technique that encrypts and decrypts data with a single key. 128-, 192, or 256-bit keys are used in a 128-bit block cipher. Because of its great flexibility and safety, it is perfect for specialized hardware, 8-bit smart card microprocessors, and huge microprocessors.

Two fish is characterized by a rather complex key scheduling and the usage of pre-computed key-dependent S-boxes. The encryption technique is modified using the other half of ann-bitkey (key-dependent S-boxes), while the other half of the key is utilized as the actual encryption key.

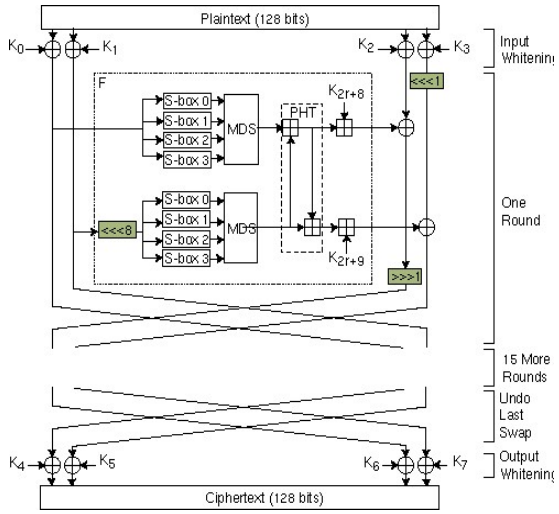


Figure 4: Twofish

METHODOLOGY

The primary goal of methodology is offering higher security to our system as well as to the sensitive data. Therefore, the solution is to leverage blockchain technology and some kind of algorithmic rule coding to prevent attacks.

In addition to blockchain technology, this solution introduces two levels of authentication. Hybrid encryption is primary level of encryption, is used to the user's authorization and authentication. Second

level is the face recognition is used to identify the authentication of the owner of the system. The select two authentication systems may beable to store wind as well as share data using the blockchain technique when they start to change their functionalities. Every piece of data is stored in an encrypted format. When the system is disabled, an outsider utilizing it is unable to determine what information was entered into the system.

The system's architecture diagram is displayed below. The system is primarily a form of encryption software that may be used personally by any user or business. The system is described as follows:

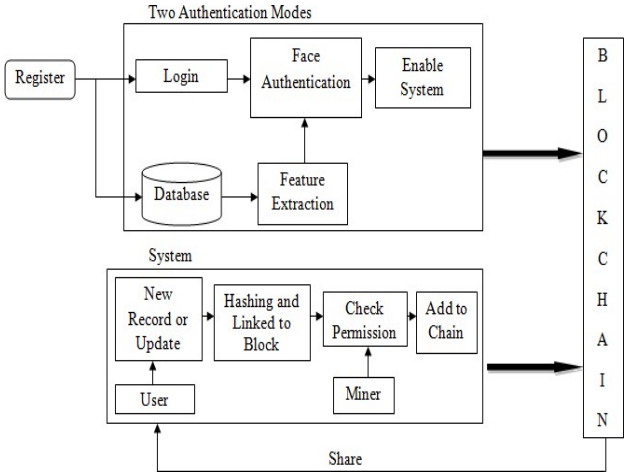


Figure 5: System Architecture

A. Two modes of authentication

Sometimes called to as double factor verification or two-venture confirmation, two-factor validation (2FA) is a security cycle in which users provide two different confirmation variables to verify themselves. Both the client's qualifications and the assets they can access are never truly assured by this cycle. Compared to verification methods that use single-factor confirmation (SFA), where the client provides just one factor - typically a password or secret word two-factor validation offers a significantly higher level of security. In addition to a second factor, usually a security token or a biometric element, such as a fingerprint or facial scan, two-factor verification methods rely on the user providing a secret key.

Authentication of Users

The initial step of the system is the login phase, when the user must sign in to the system in order to do their task. The login system was created using a hybrid cryptosystem, which combines symmetric and asymmetric algorithms, such as diffie hellman key exchange and two fish, respectively, because it is based on security encryption.

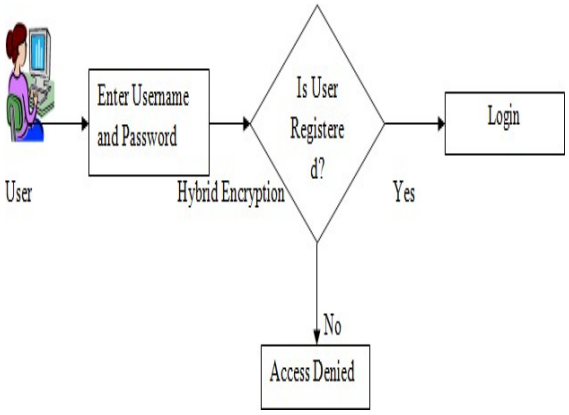


Figure 6: UserCredential

An asymmetric key exchange is used to start the interaction, in which one of the participants (the initiator) generates a random session key. A one-time session key is created using the recipient's public key and the public key of the person they need to hash (encrypt).Since the session key is now encoded, it usually transmits securely without anyone detecting it and having the ability to un scrambled (or decrypt) any communications that occur. After receiving the encrypted data, the recipients can decode it using their own private key and the symmetric encryption key that the sender was trying to teach them. In order to confirm that they have the correct key, they will then transmit a scrambled (encrypted) check message, which is encoded using a symmetric key. They will unscramble the confirmation message once it has been returned to the original sender. In the unlikely event that they are successful in decoding it, they secure the data and discover that the interaction functions correctly.

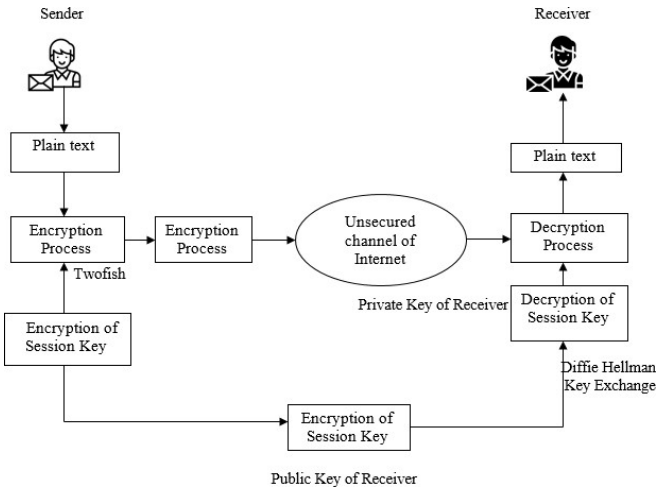


Figure7: Hybrid Encryption

Face Authentication

In order to appropriately enable the system,face recognition is the second phase.

Following that phase, the system would detect whether the owner was utilizing the software for functional purposes.

Face recognition is a biometric technique that uses particular physiologic features to identify an individual. Considering soft ware variations, facial recognition trends often follow these three steps:

1. The webcam detects the face.
2. At that time, the programming estimates a variety of facial features known as milestone or nodal foci. This could include the distance from the brow jaw line, the width of the nose, the depth of the eye attachment, and the distance between the eyes. Distinct nodal focuses are used by each program, and it will gather up to 80 various estimates for a numerical expression that addresses your unique facial mark.
3. A data set is now acquired once the face mark is analyzed. All of this might happen in just one second.

Authorities frequently used facial recognition software to identify suspects in the field. The areas of security and well-being are crucial for facial recognition. Face recognition systems can be used to identify people in images, videos, or continually. Cell phones may also be used by law enforcement to identify people during traffic stops. Face recognition has been used to target participants in assured discussions.

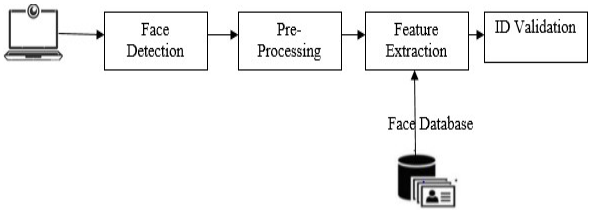


Figure 8: Face recognition diagram

A. Blockchain Technology

The term "blockchain" refers to a whole system of appropriated ledger technologies that have been changed to record and track everything, including financial transactions, medical records, and even land titles. A blockchain could be a data-containing network of squares. Blockchain might be a distributed technology that is completely accessible to everyone.

Blockchain may be a cutting-edge record that is currently gaining a lot of attention and traction. One important aspect of the business is keeping track of information and interactions. This information is often handled internally or provided to an outside party, such as representatives, financiers, or legal counsel, which increases the business's time, expense, or both. Fortunately, Blockchain avoids this drawn-out process and promotes the exchange's faster development.

Permissioned Blockchain

A permissioned blockchain could be a collection of blockchain with only relevant hubs where all of the organization's members are identified. This adds an additional degree of security to the blockchain. Blockchain networks that require admission to participate are known as permissioned blockchain. An effect layer that integrates the actions of the authorized members

operates on top of the blockchain in these kinds of blockchain.

As you can see, permissioned block chains function completely differently from both public and individuals blockchains. They are designed to provide the benefits of blockchain technology without losing the robustness of a uniform architecture. Furthermore, private blockchains, which grant newly established hubs permission to participate in the company, are distinct from permissioned blockchains. For instance, a bank might also be operating a separate blockchain that is operated through a specific number of internal hubs. It's interesting to note that permissioned blockchains might allow anyone to join an organization if their qualifications and character are established.

The distributed ledger, immutability, and consensus system properties are maintained via permissioned blockchain. Permissioned blockchains are approved by the individuals within the organization. In any event, the members of the organization should share the data on a permissioned blockchain. As a result, the subject of protection comes up. Information security and protection could be resolved since the data should be distributed among the hubs.

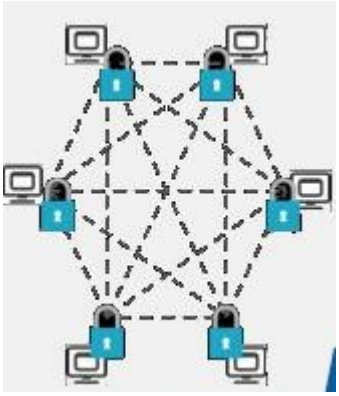


Figure 9: Permissionned Blockchain

Conclusion

Based on the research, we have a better understanding of how current technology is creating complex security. Lastly, cryptography techniques are used in all technologies to create security. The most crucial steps are encryption, key creation, and decryption. Each encryption technique uses a different approach. The three techniques used in this paper's concept for authorization and authentication are face detection authentication and hybrid encryption. Each type of technology begins with the degree of authentication and the complexity of every stage that ensures the security of a large amount of data or sensitive information. Blockchain is the primary trending technology at every level. The system would be more secure than we anticipated in addition to the blockchain employing certain sophisticated encryption techniques, such as double or hybrid encryption.

References

1. Itisha Jain, Blockchain Technology and Cryptography, International Journal of Science and Research (IJSR), Volume 13 Issue 5, May 2024. DOI: https://dx.doi.org/10.21275/SR24524003904.
2. Chandan Kalita, Sikdar Md S. Askari, Mirzanur Rahman, Rabinder Kumar Prasad, Bikramjit Choudhury and Moirang them Tiken Singh, A Novel Blockchain- Based Approach for Secure and Efficient Database Management, International Journal of Intelligent Systems And Applications In Engineering-2024.
3. Asma Mubark Alqahtani, Abdulmohsen Algarni, A Survey on Blockchain Technology Concepts, Applications and Security, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 14, No. 2, 2023.
4. Sartaj Ahmad and Sanjeev Kumar Dwivedi, Study of Cryptographic Techniques Adopted in Blockchain, Conference Paper · May 2023 DOI: 10.1109/ICIEM59379.2023.10166591.
5. Sheping Zhai, Yuanyuan Yang, Jing Li, Cheng Qiu and Jiangming Zhao, Research on the Application of Cryptography on the Blockchain, IOP Conf. Series: Journal of Physics: Conf. Series 1168 (2019) 032077 IOP Publishing,doi:10.1088/17426596/1168/3/032077.
6. Rajesh Kumar Sharma and Ravi Singh Pippal, Blockchain-based Efficient and Secure Peer-to-Peer Distributed IoT Network for Non-Trusting Device-to- Device

7. Communication, https://doi.org/10.31449/inf.v47i4.3494,2021.
8. R. P. Puneeth and G. Parthasarathy, Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System, International Journal of Engineering, IJE TRANSACTIONS B: Applications Vol. 36, No. 05, (May 2023) 925-933.
9. Mohamed abdelrahman, Blockchain Cryptography And Security Issues, International Journal Of Computer Science And Engineering Survey (IJCSES), vol.13, no.5/6, december 2022.
10. Priya.M andViji.K, Next-Generation Defense Security: Blockchain, IoT, Digital Twin, and Face Recognition-Based Smart Monitoring System, Volume 10, Issue 1, January – 2025 International Journal of Innovative Science and Research Technology, ISSN No:-2456-2165, https://doi.org/10.5281/zenodo.14621435.

******