The book proposes a framework called Sec Net for ensuring the safety of data over its lifecycle via the Internet at scale. The widespread dispersion of data across digital spaces has rendered authentication and authorization of its usage difficult. The proposed architecture is comprised of three primary elements: To generate authentic big data, block chain-based data exchange with ownership guarantee is necessary. Block chain technology makes it possible to verify the authenticity of the data and trace it back to its original creator. Data encryption enabled by artificial intelligence: This system has the potential to create a more secure and trustworthy digital ecosystem by developing more nuanced security rules. When used to cyber security, AI has the potential to discover new vulnerabilities and flaws in the system. The effectiveness of AI may be improved if individuals were incentivized to share their data via the establishment of a trustworthy system for exchanging monies in exchange for the supply of a security service. This book compares the typical Sec Net implementation with some of its alternatives.

Dr.B.Hari Krishna Associate Professor CSE at Malla Reddy Engineering College, having 10 years of teaching experience
Dr Syed Jalal Ahmad Professor CSE at Malla Reddy Engineering College, having 21 years of teaching experience
Dr. Patnala S. R. Chandra Murty Professor& HOD CSE at Malla Reddy Engineering College, having 15 years of teaching experience

9 786206 782117

B. Hari Krishna
Syed Jalal Ahmad
P.S.R Chandra Murty

DATA SECURITY USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

Network Security

LAP LAMBERT Academic Publishing

B. Hari Krishna
Syed Jalal Ahmad
P.S.R Chandra Murty

DATA SECURITY USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

B. Hari Krishna
Syed Jalal Ahmad
P.S.R Chandra Murty

DATA SECURITY USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

Network Security

LAP LAMBERT Academic Publishing

Imprint
Any brand names and product names mentioned in this book are subject to trademark, brand or patent protection and are trademarks or registered trademarks of their respective holders. The use of brand names, product names, common names, trade names, product descriptions etc. even without a particular marking in this work is in no way to be construed to mean that such names may be regarded as unrestricted in respect of trademark and brand protection legislation and could thus be used by anyone.

Cover image: www.ingimage.com

Publisher:
LAP LAMBERT Academic Publishing
is a trademark of
Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L publishing group

120 High Road, East Finchley, London, N2 9ED, United Kingdom
Str. Armeneasca 28/1, office 1, Chisinau MD-2012, Republic of Moldova, Europe
Printed at: see last page
ISBN: 978-620-6-78211-7

DATA SECURITY
USING
BLOCKCHAIN
AND
ARTIFICIAL INTELLIGENCE

ABSTRACT

The book proposes a framework called Sec Net for ensuring the safety of data over its lifecycle via the Internet at scale. The widespread dispersion of data across digital spaces has rendered authentication and authorization of its usage difficult. The proposed architecture is comprised of three primary elements: To generate authentic big data, blockchain-based data exchange with ownership guarantee is necessary. Blockchain technology makes it possible to verify the authenticity of the data and trace it back to its original creator. Data encryption enabled by artificial intelligence: This system has the potential to create a more secure and trustworthy digital ecosystem by developing more nuanced security rules. When used to cyber security, AI has the potential to discover new vulnerabilities and flaws in the system. The effectiveness of AI may be improved if individuals were incentivized to share their data via the establishment of a trustworthy system for exchanging monies in exchange for the supply of a security service. This article compares the typical Sec Net implementation with some of its alternatives. We also analyzethe repercussions on network security and revenue generation. Overcoming the challenges of allowing data interchange through the internet is central to the proposed architecture, which aims to boost AI performance utilizing real-world huge data.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVATION	FULL FORM OF ABBREVATION
CPS	Cyber, Physical and Social
AI	Artificial Intelligence
NLP	Natural Language Processing
PDC	Personal Digital Clone
UDI	Uniform Data Identifier
RFID	Radio Frequency Identification
IoT	Internet Of Things
ML	Machine Learning
SecNET	Secure Networking
IDS	Intrusion Detection System
RSU	Road Side Unit
AIDS	Adaptable Intrusion Detection System
RDBMS	Relational Database Management System
PII	Personally Identifiable Information
PDC	Private Data Centres
SHA	Secure Hash Algorithm
IDE	Integrated Development Environment
MVC	Model, View, and Controller
ORM	Object-Relational Mapping

HTTP	HyperText Transfer Protocol
HTML	HyperText Markup Language
URL	Uniform Resource Locator
QTP	Quick Test Professional
UFT	Unified Functional Testing
API	Application Programming Interfaces
TF	Tensor Flow
CI	Continuous Integration
CD	Continuous Deployment
DDoS	Distributed Denial-of-Service
I&T	Integration And Testing
IPFS	Interplanetary File System
POW	Proof of Work
POS	Proof of Stake

CHAPTER-1

INTRODUCTION

The integration of cyber, physical, and social (CPS) systems is becoming increasingly prominent in the advancement of information technology, aiming for a cohesive information society rather than a purely digital Internet [1]. In the current digital era, individuals should ideally have complete autonomy over their data usage, but the reality is quite different. The significance of data in today's information culture has incentivized major corporations to amass vast quantities of it [4, 5]. Presently, significant multinational corporations are amassing substantial amounts of personal data from their clientele, encompassing online conduct, contacts, preferences, and mobility, through the integration of embedded sensors in their devices (references 6 and 7). Given the absence of an infallible approach to supervise data access, individuals who own the data are deprived of authority over determining who can gain access to their information.

Consequently, the existing systems to identify and penalize perpetrators of data theft are inadequate [8]. Poorly managed data risks can be challenging to address [9]. For instance, when an organization acquires individuals' personal data on a large scale, it diminishes their ability to comprehend and manage associated risks. Moreover, the potential for misconduct increases when records cannot be altered.

The significance of data in contemporary information culture has incentivized prominent corporations to amass substantial quantities of it [4, 5]. Multinational enterprises are progressively collecting vast amounts of personal data from their customers, including online behavior, contacts, preferences, and movements, by utilizing embedded sensors in their devices (references 6 and 7). Given the absence of a completely dependable method to monitor data access, individuals who own the data have limited authority over its availability. As a result, the current systems designed to identify and punish data theft offenders are inadequate [8]. Poor management of data risks presents notable challenges [9]. For instance, when a large organization procures personal data from individuals, it diminishes their ability to fully comprehend and regulate the associated risks. Additionally, the unalterable nature of records further

heightens the potential for malicious activities, Artificial intelligence (AI) is the replication of human intelligence in devices that have been trained to reason, pick up new skills, and carry out jobs that traditionally call for human intelligence. It entails creating algorithms and computer systems that can process data, spot patterns, make judgments, and change their behavior in response to experience, just like people can.

A variety of tasks, including speech recognition, natural language processing, picture and video analysis, problem-solving, decision-making, and more, can be accomplished by AI systems. These systems replicate human intelligence and develop over time using a variety of techniques, including as machine learning, deep learning, neural networks,and expert systems.

The ultimate goal of AI is to develop robots that can not only mimic human thought processes but also outperform humans in particular skill sets. This will increase productivity, automate processes, and enhance problem-solving abilities in a variety offields and applications.

Given the establishment of a dependable and efficient approach to gather and consolidate data across the entire CPS, artificial intelligence (AI) exhibits the potential to proficiently manage substantial volumes of information, encompassing comprehensive data sets, resulting in the creation of authentic big data. Reference [11] highlights the significant advantages of AI advancements, such as enhanced data security and superior performance in various domains compared to human capabilities. Furthermore, research mentioned in [12] suggests that even rudimentary AI systems like the perceptron, developed in the 1950s, can outperform contemporary state-of-the- art technologies when presented with enormous volumes of data on a significantly larger scale. However, the main challenge lies in ensuring secure communication [13]. One potential solution in this context could be the integration of block chain, which employs network-wide consensus mechanisms to facilitate immutable data exchange and offers monetary incentives [14, 15]. Consequently, the utilization of block chain could provide a secure data exchange environment that benefits AI systems [16, 18]. This, in turn, has the potential to enhance data throughput and safety with the assistanceof AI.

Block chain is a distributed and decentralized digital ledger technology that

makes it possible to record transactions across a network of computers in a secure and transparent manner. A chain of blocks is created on a block chain by grouping transactions into units called blocks and connecting each block to the one before it usingcryptographic hashing.

Block chain, initially created for digital currencies such as Bit coin, is a decentralized and unalterable digital ledger that documents transactions across numerous computers.It uses cryptographic algorithms to ensure the integrity and transparency of data. Block chain's decentralized nature makes it highly resistant to tampering, fraud, and unauthorized modifications, providing a robust foundation for securing data.

By offering secure and transparent solutions for supply chain management, healthcare, banking, voting systems, and other areas, it has the potential to revolutionize a numberof different industries.

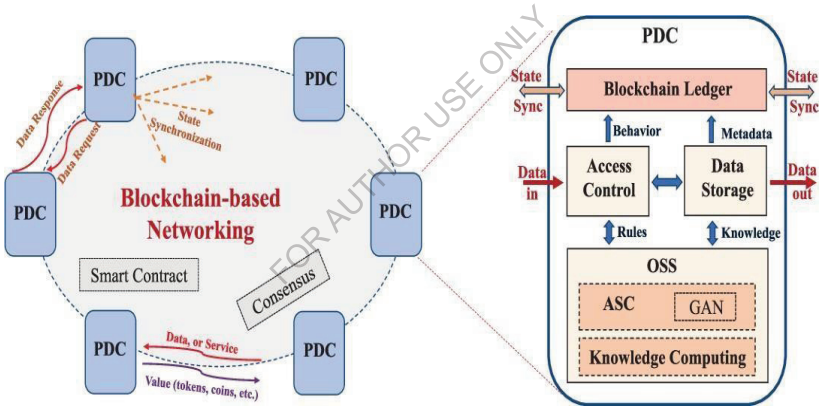

Fig 1.1 Block Diagram

The combination of block chain and AI in securing data offers several benefits. To beginwith, the inherent immutability of block chain guarantees that once data is recorded, it remains unchangeable and cannot be deleted without unanimous agreement among the participants of the network. This feature provides strong data integrity and protection against unauthorized modifications.

The integration of block chain and AI enables secure data sharing while

preserving privacy. AI techniques, such as holomorphic encryption and multi-party computation,can be utilized to encrypt sensitive data before storing it on the block chain. This featureenables authorized entities to carry out computations on encrypted data while preserving confidentiality, as the actual content remains undisclosed.

1.1 PURPOSE

1.1.1 PURPOSE OF BLOCKCHAIN

A safe, open, and decentralized system for storing and verifying transactions or data is what block chain aims to deliver. Although it was first launched as the foundation technology for the virtual currency Bit coin, its potential uses now go well beyond virtual currencies.

Each block in a chain of blocks created by block chain contains a list of transactions orother data and is created using cryptographic algorithms. Without agreement from the vast majority of network users, it becomes nearly hard to change or erase data once it has been captured in a block. The possibility of fraud or manipulation is decreased by its immutability, which guarantees data integrity.

Block chain runs on a decentralized network of computers called nodes, in contrast to conventional centralized systems. Because there is no longer a requirement for a centralized authority, the system is more robust, transparent, and resistant to single points of failure.

All users of the network can see all transactions that have been recorded on a block chain. As a result of everyone being able to independently confirm the accuracy and legitimacy of the data without depending on a third party, there is an improvementin confidence and accountability.

Block chain is extremely secure due to its distributed architecture and cryptography techniques. Only valid transactions are uploaded to the block chain because they are linked cryptographically and verified by a consensus mechanism.

Smart contracts are supported by Ethereum and other block chain platforms. Self- executing contracts with established terms and conditions are known as

smart contracts. They make it possible for automatic, trustworthy agreement execution, which lessens the need for middlemen and boosts productivity across a range of businesses.

1.1.2 PURPOSE OF ARTIFICIAL INTELLIGENCE

The goal of artificial intelligence (AI) is to build smart machines or systems that are capable of carrying out operations that traditionally call for human intelligence. Artificial intelligence (AI) tries to mimic or emulate human cognitive abilities such as perception, learning, problem-solving, and decision-making.

Artificial intelligence (AI) is intended to automate boring and repetitive processes, freeing up human resources to concentrate on more imaginative and strategic work. This boosts production and efficiency across a range of businesses.

In comparison to conventional approaches, AI can analyze enormous amounts of data, spot patterns, and derive insights to tackle complicated issues. AI algorithms are capable of resolving complex problems in a variety of industries, including transportation, banking, and healthcare.

AI makes it possible for machines to comprehend and interpret human language, which is essential for applications like language translation services and virtual assistants likeSiri and Alexa.

By using historical data to predict future events, AI helps organizations plan ahead andanticipate client wants.

Robotics is based on AI, which enables machines to see and communicate with the physical environment on their own. This has uses in the manufacturing, healthcare, andspace exploration sectors.

The ultimate goal of artificial intelligence is to enhance human talents, enhance quality of life, and solve complicated problems in a variety of fields. Ethics, openness, and responsible development are becoming more and more crucial as AI develops in orderto guarantee that AI technologies are beneficial to society.

1.1.3 PURPOSE OF SECURING DATA OVER NETWORK USINGBLOCKCHAIN AND AI

The purpose of securing data over network using block chain and AI is to protect sensitive information and ensure its integrity, confidentiality, and availability in adecentralized and automated manner.

Block chain technology provides a transparent, tamper-proof, and decentralized platform for securely storing and managing data. It ensures that data cannot be alteredor manipulated without consensus from the network participants, making it highly secure and trustworthy. AI techniques, such as machine learning and data analytics, enhance data security by detecting anomalies, identifying patterns, and automating security measures. AI can help in detecting and preventing unauthorized access, identifying potential threats or attacks, and improving overall data protection. By combining block chain and AI, organizations can establish a robust and resilient system that safeguards data against unauthorized access, tampering, or loss. It enables enhanced security, transparency, and trust in data transactions, ensuring that sensitive information remains secure and reliable.

1.2 SCOPE

1.2.1 SCOPE OF BLOCKCHAIN

The applications and uses of block chain technology are numerous and are constantly growing. Block chain has the ability to completely change how we communicate, conduct business, and share information since it is a secure and decentralized digital record.

With the introduction of crypto currencies like Bit coin, block chain became more well- known. Cross-border payments that are quicker and more secure, smart contracts for automated and transparent transactions, and improved identity verification and fraud prevention are just a few examples of its financial sector applications.

Block chain gained popularity with the advent of crypto currencies like Bit coin. A few examples of its financial industry uses include faster and more secure

cross-border payments, smart contracts for automated and transparent transactions, and enhanced identity verification and fraud protection.

Block chain technology is being investigated to maintain electronic health records securely, enabling access to and sharing of private medical data by patients and healthcare professionals. Additionally, it helps facilitate clinical studies, track pharmaceutical supplies, and improve system interoperability.

By ensuring transparency, auditability, and tamper resistance, block chain-based votingsystems can improve the integrity of elections and boost voter confidence.

Block chain is employed in the gaming industry to produce digital goods and objects that gamers may buy, sell, trade, and trade outside of the game environment, giving in-game goods true ownership and value.

1.2.2 SCOPE OF ARTIFICIAL INTELLIGENCE

The application of artificial intelligence (AI) is broad and keeps growing as technology advances. The goal of the multidisciplinary field of artificial intelligence (AI) is to develop devices, programs, or systems that can carry out tasks that ordinarily require human intelligence.

Machine learning is a branch of artificial intelligence that focuses on creating algorithms that let machines learn from data and get better over time. Unsupervised learning, reinforcement learning, and supervised learning all fall under this category.

NLP gives computers the ability to comprehend, decipher, and produce human language. Applications include sentiment analysis, language translation, and catboats and virtual assistants.

Robotics and AI are used to produce autonomous, intelligent devices that can carry out activities in a variety of fields, including industry, healthcare, agriculture, and space exploration.

AI can be used to create expert systems that mimic human proficiency in particular fields, aiding experts in their decision-making processes.

By assisting in disease diagnosis, medication research, personalized treatment, and medical picture analysis, AI is revolutionizing healthcare.

By regulating energy use, enhancing urban planning, and optimizing traffic

flow, AI can help create smarter cities.

1.2.3 SCOPE OF SECURING DATA OVER NETWORK USINGBLOCKCHAIN AND AI

The scope of securing data with block chain and AI is continuously expanding as new technologies, regulations, and threats emerge. It requires a holistic approach that encompasses technical implementation, governance, user education, and ongoing monitoring and adaptation to address evolving security challenges.

- Data Protection: Securing sensitive information and preventing unauthorized access or manipulation. This applies to personal data, financial records, medical information, intellectual property, and more.
- Transparent Transactions: Enabling transparent and traceable data transactions, ensuring accountability and preventing fraud or tampering. Block chain provides animmutable and auditable record of data transactions.
- Decentralized Security: Moving away from traditional centralized systems and adopting decentralized approaches where data is distributed across multiple nodes. This increases resilience against attacks and reduces single points of failure. Privacy Enhancement: Implementing privacy-preserving techniques to protect userprivacy while still benefiting from the transparency and security of block chain. This involves encrypting or anonym zing sensitive data.
- Fraud Detection and Prevention: Utilizing AI algorithms to identify patterns, anomalies, and potential security breaches. AI can analyze large volumes of data to detect fraudulent activities and take proactive measures to prevent them.

- Compliance and Regulation: Meeting regulatory requirements and ensuring compliancewith data protection and privacy laws. Block chain and AI can assist in maintaining audit trails, demonstrating data provenance, and adhering to legal frameworks.
- Industry Applications: The scope extends across various sectors, including finance, healthcare, supply chain management, government, energy, and more. Each industry can leverage block chain and AI to address specific data security

challenges.

- Trust and Collaboration: Building trust among stakeholders and enabling secure collaboration by ensuring the integrity and authenticity of shared data. Block chain and AI facilitate transparent and secure data sharing across multiple parties.
- Operational Efficiency: Streamlining data transactions, reducing reliance on intermediaries, and automating processes using smart contracts and AI. This leads tocost savings, faster transactions, and improved overall efficiency.

CHAPTER-2

LITERATURE SURVEY

2.1 ASSOCIATED WORK

[1] The present study describes the composition of Hyper Net, which consists of three key components: the intelligent Personal Digital Clone (PDC) representing an individual, the decentralized trusted connection established through block chain and smart contracts, and the UDI platform facilitating secure management of digital objects along with an identifier-driven routing mechanism. Hyper Net possesses the ability to safeguard data sovereignty and holds promising potential for transitioning the existing communication-centric information system into a future-oriented, data-driven information society.

[2] Utilizing the RFID system in the healthcare sector presents a viable solution to address the issue of medical privacy. By employing RFID tags within the system, valuable information can be gathered, and data exchange and processing can be facilitated with a back-end server through a reader. Throughout the entire process of information interaction, encryption techniques are predominantly employed, ensuring the confidentiality of the transmitted data. Within the framework of the Internet of Things (IoT), this paper proposes a lightweight scheme aimed at safeguarding medical privacy through the implementation of RFID technology.

[3] The prevalence of user-generated content on the Internet is on the rise; however, existing web applications confine users' data within specific boundaries, limiting sharing and integration across different services. Our belief is that users should have the seamless ability to share their data across applications and with fellow users. In light of this, we propose a framework called Amber, which separates users' data from applications while equipping applications with robust global queries to locate user data efficiently. We showcase how multi-user applications, like e-mail, can leverage these global queries to effectively gather and monitor relevant data generated by other users. By empowering users to determine which applications have access to their data and with whom it can be shared, Amber dismantles the artificial barriers that traditionally separate users' data based on applications. This not only puts users in control but also unlocks a new realm of applications that were previously

hindered by the Compartmentalization of user data [4], the task of safeguarding vast volumes of data presents a formidable challenge for the ever-increasing number of organizations engaged in its collection, storage, and monetization. To mitigate risks, it would be beneficial for these organizations to differentiate between essential data and the surplus data collected "just in case," thereby reducing the exposure to potential attacks. One possible approach is to monitor data usage and retain only the working set of actively utilized data in easily accessible storage, while securely storing the unused data elsewhere. However, this approach encounters a hurdle when it comes to big data applications that rely on periodic retraining of machine learning (ML) workloads, as the entire data store must be accessed, thereby increasing vulnerability to attacks. To address this, training set minimization techniques, such as count fraternization, are commonly employed to limit the amount of data required for training ML workloads, thereby improving performance and scalability. In our study, we introduce Pyramid, a data management system that builds upon count fraternization to enhance data protection while minimizing exposure. Pyramid uniquely presents the concept and proof-of-concept for leveraging training set minimization methods to bring rigor and selectivity to the management of big data. We seamlessly integrated Pyramid into Spark Velox, a framework utilized for ML-based targeting and personalization. Through evaluation across three applications, we demonstrate that Pyramid achieves comparable results to state-of-the-art models while training on less than 1% of the original raw data. The notion of an open data market involves establishing a framework for data trading within the realm of the Internet of Things (IoT), facilitating the exchange of data among different entities. The objective of these markets is to enable the exchange of data acquired through Internet of Things (IoT) products and solutions. Individuals who possess data ownership will gather information through Internet of Things (IoT) products and solutions, while potential data consumers will partake in negotiations with the data owners in order to gain access to the desired data. Through the utilization of data collected by Internet of Things (IoT) devices, those who consume the data can extract valuable observations regarding the preferences and behaviors of data owners. They can then leverage various methodologies to generate additional

business value, including but not limited to waste reduction and the provision of personalized services. Within open data markets, data consumers possess the chance to distribute a portion of the value generated with the data owners. Nevertheless, the issue of privacy becomes prominent when engaging in data transactions that may expose sensitive personal information. This study investigates the significance of privacy within the Internet of Things (IoT) realm, specifically in open data markets, and conducts a comprehensive analysis of existing strategies and design methodologies aiming to uphold privacy during the entirety of the data trading procedure. Furthermore, we confront critical research obstacles that must be addressed in order to transform the concept of open datamarkets into a tangible reality while ensuring the privacy protection of all parties involved.

[4] Intelligent IOT(Internet of Things) systems play a crucial role in the advancement of the next-generation Internet by integrating knowledge from the surrounding environment. These systems typically gather data from diverse dimensions through multiple devices, resulting in linkable data that holds the potential for deriving valuable insights. However, there is a risk of malicious third parties gaining access to the collected data and exploiting it to expose sensitive information. This study aims to investigate the privacy implications related to linkable data in smart IoT systems, which has not received sufficient attention in previous scholarly works. The primary focus is to explore the diverse data sources within smart IoT systems and their interconnectedness. Additionally, an extensive analysis is conducted on the potential third parties that could access and exploit this linkable data. The study thoroughly examines the potential risks and threats that individuals and communities may face within smart IoT systems. Lastly, the study highlights the existing challenges and unresolved issues surrounding the protection of privacy concerning linkable data in smart IoT systems.

[5] Traceability plays a vital role in ensuring product quality control by enabling the tracking of products throughout the various stages of a supply chain. Securing traceability information is essential to establish accountability and provide valuable forensic data. However, this task presents challenges as traceability systems often need to accommodate regulatory changes and

customized inspection processes. To address the challenges, a practical traceability system called Origin Chain utilizes block chain technology. Block chains are a novel data storage solution that facilitates decentralized architectures, allowing components to reach a consensus on shared states without relying on a central integration point. The architecture of Origin Chain provides transparent and immutable traceability information, automates the verification of regulatory compliance, and fosters adaptability within the system.

[6] In the last ten years, there has been an exponential growth of intelligent mobile devices and mobile applications, resulting in a significant transformation of these devices into adaptable and extensively utilized computing platforms. The sensory data obtained from these intelligent devices plays a vital role in supporting mobile services,and it is often perceived as innocuous information that can be accessed without the need for user authorization. However, this article aims to shed light on the potential privacy concerns associated with this seemingly innocuous data. To begin with, we provide evidence that the utilization of deep learning methods enables the identification of users' tap positions on smart device screens through the analysis of sensory data. Secondly, we establish that tap stream profiles specific to different types of apps can be compiled, enabling accurate inference of a user's app usage patterns. In order to carry out our research, we gathered sensory data and mobile app usage information from a total of 102 volunteers. The experimental findings reveal that convolutional neural networks can achieve a prediction accuracy of at least 90 percent in inferring tap positions. Moreover, leveraging the inferred tap position information, it becomes possible to accurately deduce users' app usage habits and even passwords.

[7] The number of embedded sensors in our daily lives has increased exponentially as a result of the fast-moving developments in smart gadgets and the Internet of Things (IoT). With the quantity of information these sensors collect about our surrounds, we have never-before-seen chances to comprehend and better our environment in many different ways. However, the increase in smart gadgets also prompts questions about the security and privacy of the data gathered. Deep learning techniques have become effective tools for data

analysis and inference jobs in recent years. These algorithms have proven to be incredibly effective in a variety of fields, including image identification and natural language processing. This study investigates how deep learning techniques can be used to solve the issue of determining personal information from data gathered by embedded sensors in smart devices. The goal of this study is to determine whether it is possible to extrapolate sensitive information from seemingly unimportant sensor data using deep learning-based models. In the era of widely available smart gadgets, the possible consequences of such inference approaches pose important concerns about user privacy, data protection, and ethical considerations. To do this, we suggest a novel deep learning architecture created especially for the analysis of sensor data. We want to show that the suggested model can accurately infer private information even with restricted access to some sensors, which raises severe issues about data privacy in smart settings. We outline the experimental set-up and dataset utilized in this paper for developing and testing our deep learning model. We also examine the model's performance in various contexts, taking into account various sensor kinds and data gathering settings. Our findings underline the critical need for strong privacy protection methods and show how exposed embedded sensors in smart devices are to privacy violations.

[8] The sharing of medical information has been seen as a breakthrough for the identification of novel methods and treatments for treating diseases in contemporary civilizations, cultures, and organized groupings. The primary forces behind the aforementioned claim are the electronic storage, remote access, and digitization of medical data by specialists. Hospitals create these records following patient visits, making patients the exclusive proprietors of electronic medical records. Data sharing offers a compelling benefit with the onset of the digital age and the consequent collecting of enormous volumes of data that has ushered in the big data era. Business entities that gather, process, analyze, store, and share data with other interested parties with the proper incentives have been created as a result of the value of data and the value inherent in its distribution. With an emphasis on cloud storage and processing techniques, data analytics, and data provenance, this has sparked interest across a number of industries, making conventional businesses dependent on the

availability of data for their operations and survival. Many stakeholders have turned to cloud computing and storage to give adequate solutions to urgent storage and processing demands in order to meet the growing demands for Big Data storage. Users ranging from patients, medical facilities, research organizations, and large cooperatives have expressed interest in storing their collected data on cloud repositories as cloud services have grown in popularity. However, cloud service providers are required to offer beneficiaries a controlled, flexible, and cross-domain data sharing of medical data held in their repositories.

[9] The introduction sets the stage for analyzing the important impacts of combining AI techniques with the enormous amounts of data generated in the present digital era. The massive amounts of data that organizations in a number of industries are gathering and analyzing in order to obtain insightful information, enhance decision-making procedures, and reveal significant patterns and correlations emphasize the advent of Big Data as a disruptive force. The article describes how artificial intelligence (AI) technologies, such as machine learning, natural language processing, and computer vision, play a crucial role in revealing the potential concealed inside the enormous Big Data reservoirs. Data scientists and researchers are given the tools they need by AI to create sophisticated algorithms and models that can analyze and make sense of this data on a never-before-seen scale, bringing up new possibilities in fields like fraud detection, personalized recommendations, predictive analytics, and healthcare improvements.

[10] The authors of this article investigate the pivotal role that big data plays in the creation and effectiveness of machine learning algorithms and artificial intelligence (AI) systems. The authors contend that the sheer amount of data that is available has an astounding impact on the functionality and performance of machine learning models, frequently outweighing the significance of more advanced algorithms or specially created features. The phrase "unreasonable effectiveness" describes the surreal and perhaps illogical power that data-driven tactics have. The authors use several examples from diverse fields, such as speech recognition, computer vision, and natural language processing, to show how data-driven approaches perform better than conventional rule-based systems

or expert-designed algorithms. The research is important because it clarifies the crucial role that data plays in the development of contemporary AI systems and highlights the need of collecting and utilizing enormous volumes of data to attain cutting-edge performance in a variety of AI activities. The AI and machine learning communities have been profoundly impacted by this work, which has led academics and practitioners to prioritize data collection and curation in order to develop more potent and successful AI applications.

[11] Data created by various linked devices has exploded as a result of the quick development of smart cyber-physical systems. For maintaining data privacy and assuring the effectiveness of data uploading procedures, this enormous influx of data poses both difficulties and opportunities. In their upcoming publication in the IEEE Transactions on Network Science and Engineering, the authors offer a unique, efficient, and private technique for data uploading in smart cyber-physical systems to allay these worries.

[12] Strong security measures are essential to shield vehicles from cyber dangers as they grow more connected and autonomous. The complexity and risks introduced by contemporary cars may be too much for conventional centralized security solutions to handle. The authors suggest using block chain, a distributed and decentralized technology initially created for secure transactions in crypto currencies like Bit coin, to address these problems. In-depth discussion of block chain's distinctive properties, including immutability, decentralization, and transparency, which make it a good contender for boosting vehicle security, is provided in this study. In order to guarantee the integrity and privacy of data transmitted between automobiles, infrastructure, and other stakeholders within the automotive ecosystem, the authors use block chain technology to build a tamper-resistant and trustless environment.

[13] Crowd sensing applications have become a potent tool for obtaining extensive data from a wide range of contributors as a result of the quick development of mobile technology and the rising use of Internet-of-Things (IoT) devices. In order to gather useful data on many aspects of the environment, public services, and more, crowd sensing uses the collective efforts of people's mobile devices or IoT sensors. Encouraging user participation and data input is one of the main challenges of crowd sensing. Traditional

incentive systems sometimes rely on centralized administrations or outside intermediaries, which may jeopardize user confidence and privacy. Block chain technology has drawn a lot of attention in this area because of its decentralized and tamper-resistant nature, which makes it perfect for creating trustworthy reward structures that protect privacy in crowd sensing applications.

[14] Deep learning has recently revolutionized computer vision and produced outstanding outcomes on a variety of tasks. The availability of large-scale datasets is a crucial element in the success of deep learning algorithms. Deep neural networks have been shown to perform astonishingly well, and it has been suggested that this is due in part to the amount of labeled data. The authors of this study provide a thorough investigation of how data amount and quality affect deep learning model performance. They explore various data augmentation and regularization strategies while experimenting with a variety of cutting-edge architectures and datasets. They seek to shed light on the potential constraints and opportunities of data in the context of contemporary deep learning models by undertaking extensive experiments and evaluations. This work makes several important contributions, including shedding light on the generalization behavior of deep learning models with regard to data quantity and quality, offering helpful advice on how to use data wisely, and challenging accepted notions about the significance of data for the performance of deep learning algorithms.

[15] The need for reliable and effective intrusion detection systems (IDS) has increased in recent years due to the exponential rise of digital systems and networks, which has increased cyber threats and attacks. Traditional IDS solutions have proven efficient in identifying known threats, but they frequently have trouble spotting new or complex attacks. Centralized IDS systems are also vulnerable to tampering or unauthorized access and present a single point of failure. Researchers have begun investigating the combination of block chain technology and intrusion detection technologies to address these issues. Block chain is a decentralized, immutable record that uses cryptographic methods to assure data integrity, transparency, and security. Block chain was first introduced as the technology that underpins crypto currencies. The article starts out by providing an overview of the current issues traditional IDS systems are

facing, emphasizing their shortcomings in the face of highly advanced cyber threats and attacks. The basic ideas of block chain technology are then introduced, with an emphasis on its decentralization, consensus procedures, and cryptographic qualities, which make it suited for boosting the security of intrusion detection systems.

[16] A new era of intelligent transportation systems has emerged as a result of the quick improvements in vehicle technology. These systems take advantage of cutting-edge innovations like software-defined networking and edge computing to meet the growing demand for dependable and effective vehicular networks. Numerous applications, from the transmission of multimedia information to safety-critical services, have benefited greatly from the development of connected automobiles. The vehicle context, however, poses considerable difficulties due to its unpredictable network conditions, scarcity of communication resources, and strict latency requirements. Traditional centralized cloudcomputing solutions, which frequently produce significant communication overhead and increased delay, are not well-suited to handle these difficulties. The authors suggesta collaborative edge computing paradigm designed expressly for software-defined automotive networks to overcome these problems. In order to process and offload data- intensive operations closer to the data source, this architecture makes use of the computational power of edge devices, such as roadside units (RSUs) and automobiles themselves. By doing this, the suggested method decreases communication latency, maximizes the use of network resources, and improves overall service quality in vehicle Situations [17], it is feasible to build contracts that provide a reward in exchange for a trained machine learning model for a certain data set using block chain technology. Users could then train machine learning models for a reward in an unreliable manner because to this. The answer will be automatically validated by the smart contract using the block chain, thus there won't be any room for argument regarding its validity. Users thatsubmit solutions won't be exposed to the counterparty risk of not being rewarded for their labor. Anyone with access to a dataset, including software agents, can easily construct contracts.

[17] The security of computer systems and networks faces major problems due to the continually changing landscape of cyber threats. The intricacy and

complexity of contemporary cyber-attacks have highlighted limitations for traditional rule-based intrusion detection methods. As a result, to create more efficient and adaptable intrusion detection systems (IDS), researchers and practitioners have resorted to data mining and machine learning techniques. The study explores the fundamental ideas of intrusion detection and addresses the difficulties encountered in identifying various cyber-attacks that are continually evolving. The authors highlight the need for more sophisticated strategies by examining the shortcomings of conventional intrusion detection methods. These techniques should be able to adapt to changing attack patterns and identify dangers that had not yet been discovered. The authors look at numerous data mining and machine learning strategies used for intrusion detection throughout the entire research. Decision trees, neural networks, support vector machines, clustering algorithms, Bayesian networks, and ensemble methods are just a few examples of these techniques. Each algorithm is fully described, with emphasis placed on its advantages and disadvantages with regard to cyber security. The significance of real-time intrusion detection in preventing assaults in dynamic and high-throughput situations is also discussed in the study. The authors also go over the significance of feature extraction and selection for decreasing data dimensionality and boosting intrusion detection system effectiveness.

CHAPTER-3

SOFTWARE AND HARDWARE REQUIREMENTS

3.1 SOFTWARE REQUIREMENTS

- Operating System: Windows 7 or more recent version.

Depending on the system's implementation and architecture, Windows' role in safeguarding data transmitted across a network employing block chain and AI may change. Windows can take on several functions in such a configuration.

- Programming Language: Python

Due to its adaptability, simplicity, and extensive ecosystem of libraries and frameworks, Python plays a vital part in safeguarding data over a network using block chain and AI.

- IDE/Workbench: Python 3.7

When paired with block chain and AI technologies, Python 3.7 significantly contributes to network data security.

- Framework: Django

Python developers often use the Django web framework to create web applications. While Django does not directly handle blockchain or AI features, when integrated with these technologies it can play a significant role in network data security.

- Front-End: Python.

Due to its adaptability, simplicity, and extensive ecosystem of libraries and frameworks, Python plays a vital part in safeguarding data over a network using blockchain and AI.

- Web-Designing: HTML,CSS,JavaScript.

When using blockchain and AI technology, web design is essential for protecting data transmitted over a network. Web design makes sure that these technologies are successfully integrated and presented to consumers in a secure and user-friendly manner, while blockchain and AI supply the underlying security mechanisms.

- Database : MySQL

When combined with blockchain and AI technologies, MySQL is essential for protecting data over a network. Despite being primarily a relational database management system (RDBMS), MySQL can be a key part of a larger system architecture that aims to improve data security.

3.2 HARDWARE REQUIREMENTS

- Processor: Intel core i3 and above

- Hard Disk: 500GB
- RAM: 4GB or more

Chapter-4

SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

The entire cyber realm relies heavily on data, and Artificial Intelligence (AI) algorithms derive knowledge exclusively from historical data. For instance, in online shopping applications, user review data plays a crucial role for new users in making informed decisions about which products to purchase. Similar examples can be found in sectors such as healthcare, where individuals seek information about reputable hospitals, or in education, where insights are sought regarding reliable institutions. However, not all cyber data can be publicly accessible, particularly sensitive information like Patient Health Data, which encompasses details of patients' illnesses and contact details. Making such data available publicly would compromise the security and confidentiality of patients' information. Presently, service providers such as online social networks or cloud storage platforms retain various types of user data, which they may sell to other organizations for their own advantages. Regrettably, individuals possess restricted authority over their data as it is housed within servers operated by external entities.

DISADVANTAGES

Block chain technology has serious scalability problems, especially in open, permission less networks like Bit coin and Ethereum. The network's performance may deteriorate as the volume of data increases, resulting in longer transaction times and higher expenses. To keep its decentralized nature and security, blockchain networks need a lot of computational power and electricity. Concerns concerning sustainability and the environment arise as a result of the energy-intensive nature of mining or confirming transactions in proof-of-work blockchains. All organizations might not haveeasy access to the specialized knowledge and expertise needed to implement and operate a blockchain system. It may be difficult to integrate blockchain technology into current data security architecture and operations due to its complexity. While immutability and openness are benefits of blockchain, they can also be a double-edgedsword in terms of data security. The privacy and secrecy of some data, such personally identifiable information (PII), should not be exposed to the public on a blockchain.

Large amounts of data might be expensive and impossible to store directly on the blockchain. The cost of on-chain storage rises with the size of the data, making managing large volumes of data less practical.

Self-executing contracts with predetermined terms are known as smart contracts. They might be vulnerable to flaws, weaknesses, and exploits nevertheless, which could result in unforeseen consequences and security lapses.

Although immutability is a benefit of blockchain, it can also be a drawback when attempting to restore lost or damaged data. Data cannot be easily changed or withdrawn once it has been put to the blockchain, which might make data recovery difficult and time-consuming.

By incorporating AI into data security, the system may be vulnerable to new biases and sorts of attacks. Inherent biases in AI systems could result in unfair judgments or false security evaluations. Attacks directed against AI models may also jeopardize the system's overall security.

Despite the decentralized nature of blockchain, some implementations or consensus processes may eventually cause centralization. The security and integrity of the data recorded on the blockchain may be compromised if a sizable percentage of the network's resources or decision-making authority is concentrated in the hands of a small number of entities.

In some areas, legal and regulatory barriers to the use of blockchain and AI technology may exist, particularly in relation to data protection, governance, and compliance. Making sure that regulations are followed when they are changing can be a difficult job.

4.2 PROPOSED SYSTEM

To address a fore mentioned challenge, the author proposes the utilization of Private Data Centres (PDC) in conjunction with Blockchain and AI techniques to ensure the security of users' data. This approach encompasses three key functions outlined below:

- Blockchain: By employing a Blockchain-based framework, data sharing is facilitated with guaranteed ownership, enabling trusted sharing of data on a large scale to form authentic big data. Users are granted the ability to define access control, determining which users have permission to access specific data. Blockchain objects are generated for the accessed data, restricting access only to authorized users. Users can add, subscribe, and share data within the Blockchain object while granting permissions.
- Artificial Intelligence: To establish a trustworthy cyberspace, a secure computing platform powered by artificial intelligence (AI) is utilized, enabling the implementation of intelligent security protocols. Similar to the cognitive functions of the human brain, AI performs logical operations to validate whether the requesting user possesses the required permissions for accessing shared data. If the access is authorized, AI collaborates with the Blockchain to facilitate the display of the shared data. Conversely, if the request is not authenticated, it is disregarded.
- Rewards: This technique introduces a trusted value-exchange mechanism wherein users who share their data earn rewards points whenever another user accesses their data. This economic rewards system serves as a means to purchase security services, incentivizing participants to share their data or services. The rewards system promotes data sharing, ultimately leading to enhanced AI performance.

The implementation of this project utilizes the example of medical data sharing, serving as a model to construct and develop the proposed concept.

ADVANTAGES

With blockchain technology, data integrity and immutability are guaranteed. Without the agreement of the network's users, it is nearly difficult to change or tamper with data after it has been recorded on a blockchain. This feature confirms the data's validity and

assists in preventing unauthorized access. Blockchain relies on a decentralized network of nodes, therefore data is not under the control of a single entity. With fewer single points of failure due to decentralization, thenetwork is more resistant to intrusions and data breaches.

Blockchain offers transparency since all users of the network may access the data and see its history. This openness improves accountability and makes it possible for auditors to confirm the security and correctness of the data.

Security processes and procedures can be automated using smart contracts, which are self-executing contracts with predetermined criteria. AI algorithms may analyze incoming data and cause particular smart contracts to automatically perform the necessary security precautions, reducing human error and reaction times.

Algorithms using AI and machine learning can continuously analyze network traffic and data trends, recognizing anomalies and learning from typical behavior. Real-time detection of potential security breaches or suspicious activity is made easier by this feature.

Due to its distributed architecture, blockchain-based networks can defend against DDoS attacks more effectively. Through the intelligent detection and mitigation of hostile traffic patterns, AI can significantly improve DDoS security.

Blockchain technology enables secure transactions by encrypting data and limiting access. AI can help in maintaining privacy settings and access controls, ensuring that sensitive material is only shared with people who are authorized to see it.

Users no longer have to place their trust in any one organization to protect their data thanks to the combination of blockchain and AI. Without relying on a centralized authority, the network's consensus mechanism and encryption algorithms guarantee data privacy.

Data ownership can now be more user-centric and decentralized thanks to blockchain technology. Better data governance can result from giving users more control over their data by enabling them to give or remove access privileges to particular parties.

Security systems that use AI to detect and address security threats can do so automatically, cutting down on the time it takes to respond to an incident. This short response time can lessen the effect of data breaches or perhaps prevent them altogether.

Organizations can build a strong and secure data architecture that delivers unmatched protection against cyber threats and unauthorized access by combining the strengths of blockchain and AI. However, prior to incorporating these technologies into an existing network, it's crucial to take into account the specific use cases, potential restrictions, and implementation difficulties related to them.

CHAPTER-5

SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE

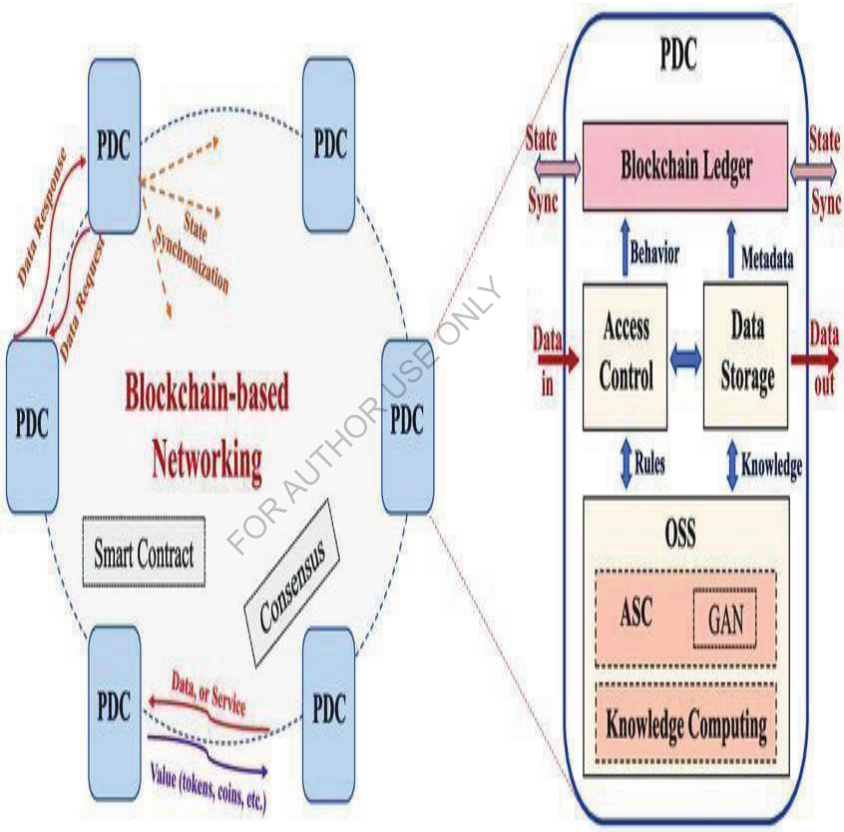

Fig 5.1 SecNet Architecture

5.2 INPUT AND OUTPUT DESIGN

5.2.1 INPUT DESIGN

The input design serves as the vital bridge connecting the information system to the user. It encompasses the formulation of specifications and procedures for data preparation, essential steps that enable the transformation of transactional data into a format suitable for processing. This transformation can occur through the computer's ability to extract data from written or printed documents, or by individuals directly inputting the data into the system. The input design primarily focuses on optimizing efficiency by minimizing required input, mitigating errors, eliminating delays and unnecessary steps, while ensuring a straightforward process. Moreover, utmost attention is given to incorporating security measures and user-friendly features while upholding privacy.

Input Design encompassed the examination of the subsequent factors:

- Input Design encompassed the examination of the subsequent factors:
- Determination of the requisite input data.
- Establishment of an appropriate data arrangement or coding scheme.
- Development of a dialogue system to facilitate guidance for operating personnel duringinput provision.
- Formulation of strategies for implementing input validations and establishing error-handling procedures.

The considerations involved in Input Design entailed:

- Identifying the specific data to be utilized as input.
- Devising an optimal structure or coding mechanism for the input data.
- Constructing a user-friendly dialogue system to aid operating personnelin input provision.
- Establishing protocols for input validation procedures and outlining the necessary stepsto be taken in the event of errors.

The elements taken into account during the Input Design phase comprised:

- Selection of the appropriate input data.
- Designing an effective arrangement or coding scheme for the data.
- Developing a user-oriented dialogue system to guide operating personnel throughout the input process.
- Establishing protocols for input validation and defining the required error-handling procedures.

In the context of Input Design, the following aspects were considered:

- Determining the specific input data to be utilized.
- Defining an optimal arrangement or coding scheme for the data.
- Creating a dialogue system to assist operating personnel in providing input.
- Establishing methodologies for implementing input validations and outliningerror resolution steps.

OBJECTIVES

Input Design involves the conversion of a user-centric input description into a computerized system, serving the purpose of preventing data input errors and guiding management towards accurate information retrieval from the computerized system.

The creation of user-friendly screens for data entry is a key aspect of achievingeffective Input Design, especially when dealing with large volumes of data. Theprimary objective is to simplify the data entry process and minimize errors. Thedata entry screen is strategically designed to accommodate all necessary data manipulations while also offering record viewing capabilities.

In the data entry stage, a validation process is conducted to verify the precision and dependability of the entered data. To facilitate this validation, screen interfaces are utilized, accompanied by timely and appropriate error messages. The aim is to assist users and avoid any potential misunderstandings. In essence, the goal of Input Design is to establish an instinctive input layout that is easily understandable and user-friendly.

5.2.2 OUTPUT DESIGN

A satisfactory outcome refers to one that fulfills the demands of the ultimate recipient and effectively conveys information. Outputs serve as a means of conveying processed results to both users and other systems within a given system. During output design, the arrangement of information for immediate access and the creation of hard copy outputs are established. Such outputs constitute the primary and vital information source for users. Enhancing the system's alignment with user decision-making is accomplished through effective and astute output design. The process of designing computer output necessitates a systematic and meticulous approach, ensuring the creation of suitable output elements that are user-friendly and efficient. During the analysis and design phase of computer output, it is crucial to identify the precise outputs required to fulfill the given requirements.

- For appropriate techniques to present information effectively.

- Generate various formats such as documents, reports, or other mediums to accommodate the information generated by the system.

The intended outcome of an information system should fulfill a set of distinct aims, which encompass the following:

- Conveying information regarding previous endeavors, present condition, or future projections.

- Signaling noteworthy occurrences, prospects, challenges, or cautionary signs.

- Initiating a course of action.

- Validating the execution of an action.

5.3 MODULE DESCRIPTION

It contains three modules in Securing Data Over Network Using Blockchain and AI. They are as follows:

PATIENTS

Patients first create his profile with all disease details and then select desired hospital with whom he wishes to share/subscribe data.

While creating profile application will create Blockchain object with allowable permission and it will allow only those hospitals to access data.

Patient can login to application with his profile id and check total rewards he earned from sharing data.

HOSPITAL

During the present era, any hospital has the ability to access an application and subsequently input a search query in the form of a disease name.

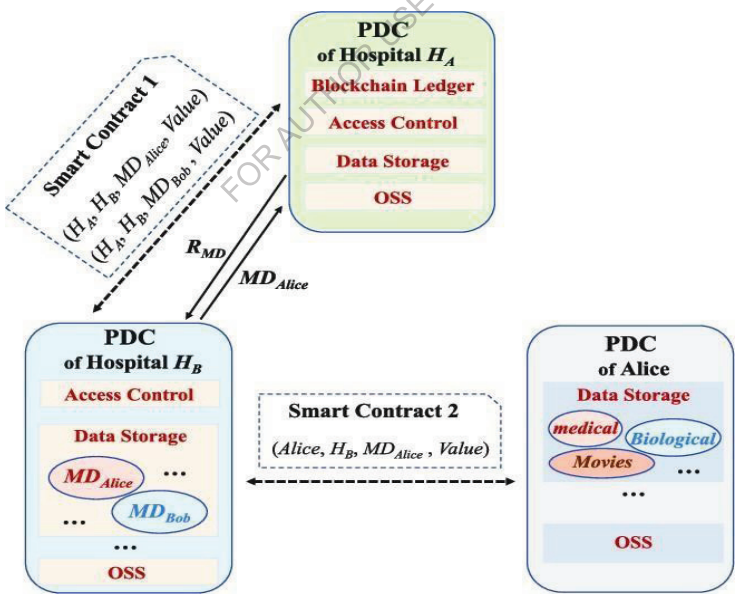

Fig 5.2 Flow Diagram of Hospital and Patients

5.4 UML Diagrams

5.4.1 CLASS DIAGRAMS

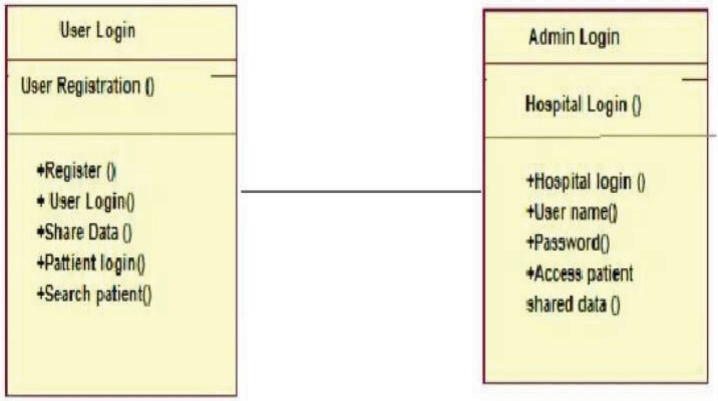

Fig 5.3 Class Diagram

USE CASE DIAGRAM

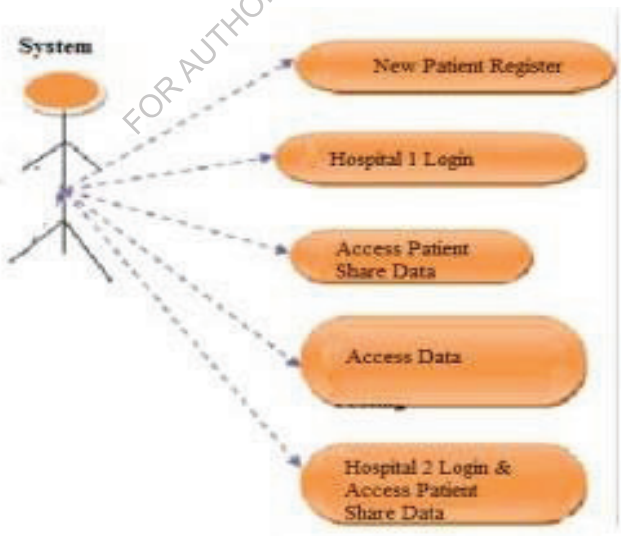

Fig 5.4 Use Case Diagram

5.4.2 SEQUENCE DIAGRAM

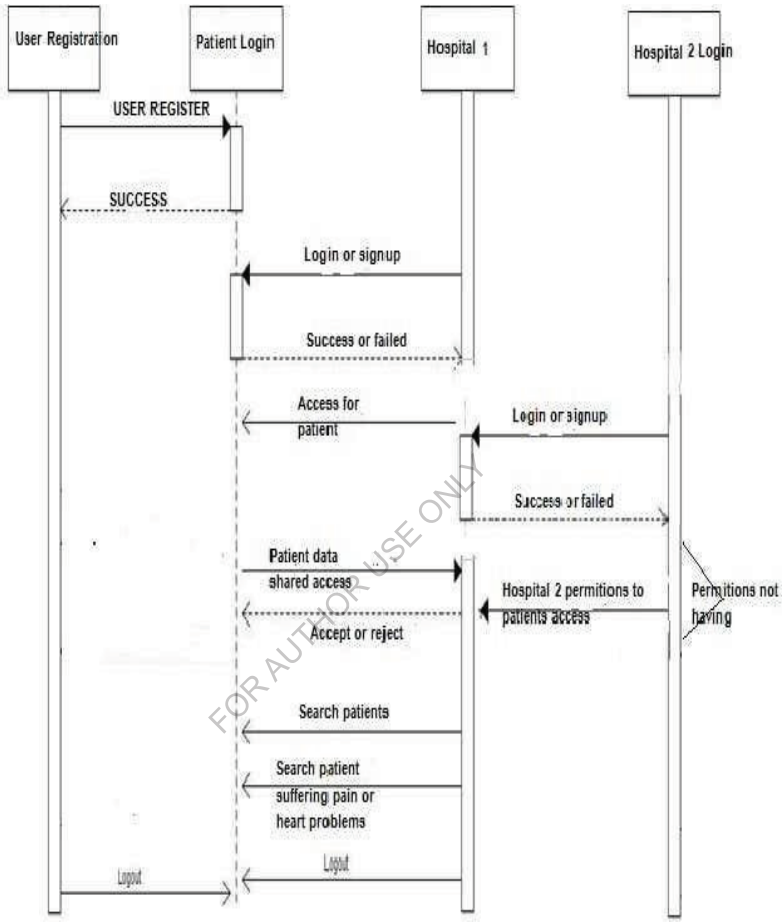

Fig 5.5 Sequence Diagram

5.4.3 ACTIVITY DIAGRAM

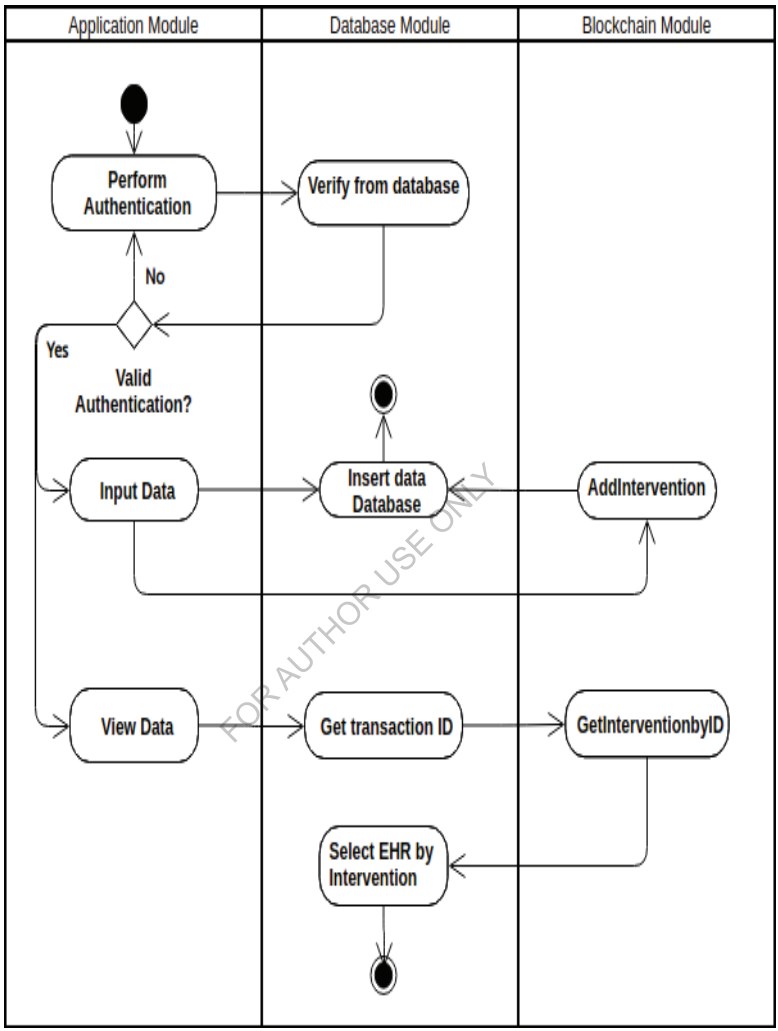

Fig 5.6 Activity Diagram

CHAPTER-6

IMPLEMENTATION

6.1 ALGORITHM USED

SHA Algorithm

The SHA (Secure Hash Algorithm) is a family of cryptographic hash functions designed to produce a fixed-size output (hash value) from any given input data. It is widely used in varioussecurity applications and protocols to ensure data integrity and provide digital signatures.

There are different variants of the SHA algorithm, including SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. The numbers represent the output size of the hash value in bits.

Use of SHA Algorithm

1. Input Data: The SHA-256 algorithm takes an input message of any length as input, whichcould be a text string, a file, or any other data.
2. Padding: The input message is padded to a specific length to meet the block size requirements of the algorithm. The padding ensures that the input message can be divided into fixed-size blocks for processing.
3. Message Digest Calculation: The algorithm processes the padded input message in blocks and performs a series of bitwise logical and arithmetic operations on the data.
4. Compression Function: SHA-256 utilizes a compression function that combines the input block with the current hash value to produce an intermediate hash value.
5. Iteration: The compression function is applied iteratively to process each block of the input message, updating the intermediate hash value at each step.
6. Final Hash Value: Once all blocks have been processed, the final hash value, also knownas the message digest, is obtained. The hash value is a fixed-size string of 256 bits (32 bytes).

The cryptographic security of the SHA-256 algorithm is well-established, as it generates a distinct hash value for every unique input message. Even a minor alteration in the input data would yield a substantially distinct hash value, rendering the process of reconstructing the original input exceedingly challenging. SHA-256 finds extensive application in numerous cryptographic uses, including digital signatures, verification of data integrity, password storage, and blockchain technology. It offers a dependable and

efficient mechanism to safeguard and maintain the integrity and security of data across various contexts.

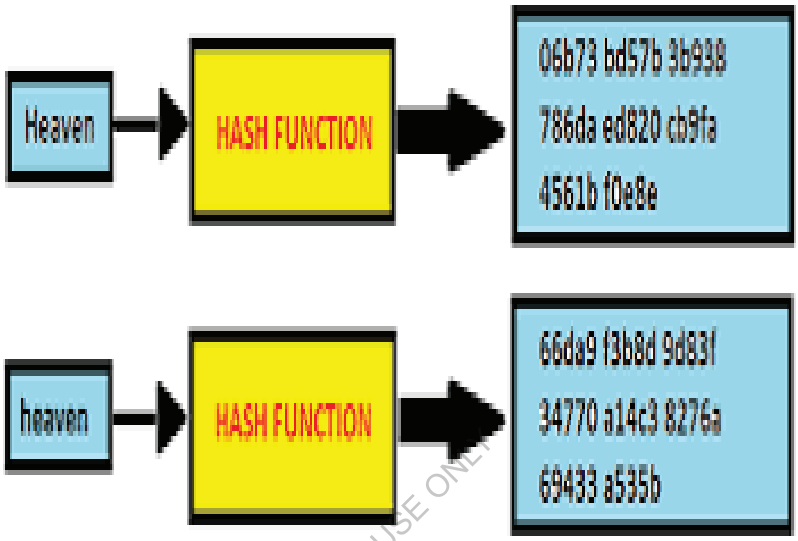

Fig 6.1 SHA Algorithm

TECHNOLOGY DESCRIPTION

6.1.1 PYTHON

Python, as a programming language, possesses remarkable versatility. It is an interpreted and interactive language that operates at a high level, incorporating an object-oriented approach. Python adheres to a design philosophy that emphasizes code readability, achieved notably through the utilization of whitespace indentation to delineate code blocks rather than relying on curly brackets or keywords. This distinctive syntax enables programmers to express concepts concisely, often resulting in fewer lines of code when compared to languages like C++ or Java. Python offers an array of constructs that facilitate clear programming on both small and large scales. It enjoys support across multiple operating systems, and its reference implementation, C and Python, is open source software, developed through a community-driven model, much

like its various implementations. The Python Software Foundation, a non-profit organization, oversees the management of C and Python. Python prides itself on its dynamic type system and automatic memory management. It accommodates multiple programming paradigms, encompassing object-oriented, imperative, functional, and procedural approaches. Furthermore, Python provides an extensive and comprehensive standard library, enhancing its capabilities further.

What is Python

Python has gained significant popularity as a programming language since its inception in 1991 by Guido van Rossum. Its versatility allows it to be applied in various domains, including software development, mathematics, system scripting and web development (server-side).

What can Python do

- Python possesses the capability to develop web applications when deployed ona server.
- Python has the potential to collaborate with software in order to establish workflows.
- Python exhibits the ability to establish connections with database systems, along with the capacity to read and manipulate files.
- Python can handle large datasets and execute intricate mathematical operations. Python provides benefits in terms of speedy prototyping and the creation of software intended for production purposes.

Why Python

- Python is versatile and can be used on multiple platforms, including Raspberry Pi, Linux, , Mac, Windows and other operating systems.
- Python possesses a straightforward syntax that closely resembles the English language.
- Python's syntax enables developers to write programs in a more concise manner, resulting in the requirement of fewer lines of code compared to certain alternative programming languages.
- Python operates on an interpreter system, allowing code execution immediately after it is written, thereby facilitating rapid prototyping.
- Python offers the flexibility to be approached and utilized in various

programming paradigms, including procedural, object-oriented, and functional approaches.

Good to know

The latest significant release of Python is Python 3, which will be utilized throughout this tutorial.

Despite Python 2 no longer receiving updates aside from security patches, it continues to maintain a considerable user base.

When working with Python code, there are multiple options for writing it. While usinga text editor alone can be sufficient, it is also feasible to employ an Integrated Development Environment (IDE) such as Thonny, PyCharm, NetBeans, or Eclipse., especially when dealing with extensive sets of Python files. This approach offers notable advantages.

In contrast to many other programming languages that frequently employ semicolons or parentheses, Python utilizes new lines to conclude a command.

Python's defining of scope, such as loops, functions, and classes, relies on indentation through whitespace, while alternative programming languages often employ curly brackets for this purpose.

Python Install

Python is pre-installed on a significant number of PCs and Macs. To confirm the presence of Python on a Windows PC, you have two options: you can search for "Python" in the start bar or execute the following command on the Command Line (cmd.exe):

```
C:\Users\Your Name>python --version
```

To check for Python installation on Linux or Mac, open the command line in Linux or the Terminal in Mac, and enter the following command:

```
python --version
```

If you discover that Python is not installed on your computer, you can freely downloadit from the following website: **https://www.python.org/**

Python Quick Start

Python falls under the classification of an interpreted programming language, wherein developers generate Python (.py) files using a text editor and subsequently run them through the Python interpreter. To execute a Python file, the following command line syntax is used: C:\Users\Your Name>python helloworld.py, where "helloworld.py" represents the specific name given to your Python file.

To begin creating our initial Python file, helloworld.py, we can utilize any text editor. Within helloworld.py, we incorporate a single line of code: print("Hello, World!"). This process is relatively simple. After saving the file, proceed to open the command line and navigate to the directory where the file is stored. Execute the command: C:\Users\Your Name>python helloworld.py. Upon execution, the output displayed will be: Hello, World!

The Python Command Line

When testing a small piece of Python code, it can sometimes be more efficient and convenient to execute the code directly in the command line without creating a separate file. This capability is enabled by Python's ability to run as a command line interface.

To accomplish this, you can follow these steps on the Windows, Mac, or Linux command line:

1. Open the command line interface. Enter the following command: **C:\Users\Your Name>python**. If the "python" command does not work, you can try using "py" instead: **C:\Users\Your Name>py**.
2. Once you have entered the appropriate command, you can start writing and executing your Python code directly in the command line interface.
3. For example, you can refer back to our previous tutorial's "hello world" example and type the following command: **C:\Users\Your Name>python**.
4. The command line interface will display the Python version you are using, along with additional information such as the system architecture.
5. You can access further information by typing commands such as "help," "copyright," "credits," or "license."

>>>print("Hello, World!")

Which will write "Hello, World!" in the command line:C:\Users\Your Name>python
Python 3.6.4 (v3.6.4:d48eceb, Dec 19 2017, 06:04:45) [MSC v.1900 32 bit
(Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Hello, World!")Hello, World
To exit the Python command line interface, you can conveniently terminate the session by entering the following command:
exit()

6.1.2 DJANGO

Django, a Python web framework that operates at a higher level of abstraction, simplifies the creation of web applications by optimizing the development procedure. Employing the Model-View-Controller (MVC) architectural paradigm, Django effectively segregates application components and fosters the reuse of code.

Here's a detailed explanation of the different components and features of Django:

- Model: The model component of Django deals with the data and the database. It provides an Object-Relational Mapping (ORM) layer that allows you to define your data models as Python classes. These classes map to database tables, and the attributes of the class represent the fields in the table. Django's ORM handles the generation of SQL queries and makes it easier to interact with the database.
- View: The view component of Django handles the logic of the application. It receives requests from the user's browser, processes them, and returns responses. Views are Python functions or classes that define the business logic for handling different HTTP requests. They can perform tasks such as retrieving data from the database, processing user input, and rendering templates to generate HTML responses.
- Template: Django uses a template system to generate dynamic HTML pages. Templates are separate files that contain HTML markup with embedded template tags. These tags allow you to include dynamic content and logic within the HTML. Django's template engine processes these templates and replaces the template tags with the actual values. This separation of concerns between the presentation and the business logic helps in maintaining clean and readable code.
- URL Dispatcher: The URL dispatcher in Django maps incoming URLs to the appropriate view functions or classes. It defines a set of rules (URL patterns) that specify how different URLs should be handled. When a user requests a URL, Django's URL dispatcher matches it against the defined patterns and routes the request to the corresponding view for processing.
- Forms: Django provides a forms framework that simplifies the handling of

HTML forms. Forms in Django are defined as Python classes that represent the structure of a form. They handle form validation, data cleaning, and provide convenient methods for rendering forms in HTML. Django's forms framework helps in reducing the amount of boilerplate code required for form handling and validation.

Overall, Django is a comprehensive web framework that enables developers to quickly build robust and scalable web applications using Python. Its rich set of features, adherence to best practices, and active community support have made it a popular choice for web development.

6.2 SAMPLE CODE

Require:

mapping (hash => struct) public Data; mapping (pubkey => int) public balance; mapping (address => hash) private reverseIndex; procedure RegisterData(hash,description,address, price)Data[hash].owner ← msg.sender Data[hash].address ← address Data[hash].description ← description Data[hash].price ← price Data[hash].subscribers ← [] reverseIndex[address] ← hash

return TRUE end procedure

procedure WithdrawData(hash)

require (Data[hash].owner == msg.sender) reverseIndex[Data[hash].address] ← NULLData[hash] ← NULL

end procedure

procedure SubscribeData(hash)

require (balance[msg.sender] >= Data[hash].price) balance[msg.sender] −= Data[hash].price Data[hash].subscribers += msg.sender

end procedure

procedure RequestDataWithAddress(address) require (reverseIndex[address] != NULL) hash ← reverseIndex[address]

require (msg.sender ∈ Data[hash].subscribers) return AccessToken for address with TTL

end procedure

procedure RequestDataWithHash(hash) require (msg.sender ∈ Data[hash].subscribers)

address ← Data[hash].address

return AccessToken for address with TTLend procedure

CHAPTER-7

SYSTEM TESTING

The primary objective of testing is to uncover any potential errors or flaws within a

work product. By systematically exploring all conceivable faults and weaknesses, testing servesto verify the functionality of individual components, sub-assemblies, assemblies, or the final product. Its purpose is to rigorously exercise software, ensuringthat the software system not only fulfils its intended requirements and user expectations but also avoids anyunacceptable failures. Various test types are available, each cateringto specific testing requirements.

Testing entails the comprehensive assessment of a system or its constituent parts, aimedat determining whether they meet the prescribed requirements. Simply put, it involves executing the system to identify any deviations, mistakes, or unmet requirements that differ from the desired specifications.

7.1 TYPES OF TESTING

7.1.1 MANUAL TESTING

The process of software testing through manual means involves a hands-on approach to gain insights and identify functionality issues. It encompasses not only the verification of specified features outlined in requirements documents but also the testers'endeavor to simulate end users'perspectives. Manual test plans range from meticulouslyscripted test cases with explicit steps and anticipated outcomes to overarching guidelines that facilitate exploratory testing sessions. Various advanced tools, such as Test Pad, are available in the market to aid in manual testing.

The manual testing of blockchain and AI-based network data security entails running a number of tests to evaluate the efficiency and dependability of the security controls putin place in the system.

KEY ASPECTS OF SECURING DATA OVER NETWORK USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR MANUAL TESTING

Make sure that sensitive data is encrypted both during transmission and when it is stored. Make sure that when authorized people access the data, the decryption procedure

functions properly.

To guarantee that only authorized individuals have access to particular data and functionality, test the access restrictions. Make sure that permissions are appropriatelygranted and removed.

If security procedures are automated by smart contracts, manually audit the code to findany flaws or potential exploits.

Test the system's response to errors, exceptions, and unexpected inputs to avoid potential security loopholes.

7.1.2 AUTOMATION TESTING

Automated software testing encompasses the utilization of specialized tools to detect software flaws, streamlining the testing process. Testers employ automation tools to execute test scripts and effortlessly generate test outcomes, eliminating the need for manual intervention. Prominentfunctional testing automation tools include QTP/UFT and Selenium.

KEY ASPECTS OF SECURING DATA OVER NETWORK USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR AUTOMATIONTESTING

Automation testing of Securing Data Over Network using Blockchain and AI involves using automated testing tools and frameworks to validate the security measures implemented in a system that combines blockchain and AI technologies. This ensures that the system is resilient against security vulnerabilities and can protect sensitive dataeffectively.

Identify the key security aspects of the system that need to be tested, such as data encryption, access controls, smart contract execution, anomaly detection, and identity management.

Choose appropriate automation testing tools that can interact with blockchain networksand AI components. Some tools may support interaction with blockchain networks using APIs, while others may simulate AI behavior for testing. If the system uses smart contracts on the blockchain, perform testing to ensure the contracts are secure, and the logic is implemented correctly. Tools like Truffle or Ethereum tester can help automate smart contract testing.

For AI components, automate the testing of machine learning models to ensure they produce accurate and reliable results. AI testing frameworks like TensorFlow's TF Testing can be used for this purpose.

Automate the testing of the AI-based anomaly detection algorithms to validate theirability to detect and respond to security threats effectively.
Test the integration of blockchain and AI components to ensure smooth data flow andsecure communication between different parts of the system.

Ensure that the system adheres to relevant industry standards and compliance requirements for data security and privacy.

METHODS OF TESTING

7.1.3 STATIC TESTING

Termed as Software Testing's Verification technique, it involves the examination of documentsand files in a static manner. This process ensures that the development aligns with the specified requirements, validating both the accuracy of the product's construction and adherence to the intended specifications. The activities encompassed within this method encompass Inspections,Reviews, and Walkthroughs.

KEY ASPECTS OF SECURING DATA OVER NETWORK USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR STATIC TESTING

To examine the source code of the blockchain and AI components, static code analysiscan be used. Security faults, such as problems with input validation, poor management of sensitive data, or potential vulnerabilities in the smart contracts,

can be found by security professionals.

For blockchain-based systems, smart contract audits are essential. Static analysis tools can be used to analyze the code of smart contracts to uncover security loopholes, potential attack vectors, or unintended behaviors.

In AI-based systems, static testing can review access control mechanisms to ensure thatonly authorized entities have access to critical data and functionalities.

Static testing can help ensure that encryption and key management practices are properly implemented to protect sensitive data both in transit and at rest.

If the system relies on APIs (Application Programming Interfaces), static analysis can be applied to the API code to verify that they are secure and not exposing sensitive dataor functionalities unintentionally.

Static testing involves examining system documentation, including security guidelines, policies, and procedures, to verify that security practices are well-documented and followed throughout the development process.

Static testing can help ensure that the system complies with relevant privacy regulations by reviewing data handling practices, consent mechanisms, and data anonymization methods.

7.1.4 DYNAMIC TESTING

Validation in software testing, also referred to as Software Testing Verification, is an essential dynamic procedure that focuses on assessing the real product. The objective of this process is toensure the accuracy and appropriateness of the developed product by validating its conformity with the intended requirements. The activities encompassed within this process primarily revolve around testing the software application.

KEY ASPECTS OF SECURING DATA OVER NETWORK USING BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE FOR STATIC TESTING

Dynamic testing involves continuously monitoring the data and network activity duringnormal operation. This monitoring can be performed using various AI-based algorithms that analyze data patterns and detect any unusual or suspicious activities.

AI-powered security systems can be trained to recognize known threats and indicators of compromise. Dynamic testing involves simulating various cyber-attacks and observing how the AI and blockchain-based security measures respond to these threats.

Dynamic testing uses AI algorithms to identify anomalies in network traffic, user behavior, or data patterns that could indicate potential security breaches. These anomalies may be indicative of cyber-attacks or unauthorized access attempts.

Stress testing evaluates the system's performance and resilience under high-load conditions. In the context of securing data with blockchain and AI, stress testing can assess how the network copes with a large number of data transactions and AI processing demands while maintaining security and integrity.

Dynamic testing involves simulating various types of attacks, such as DDoS attacks, phishing attempts, malware injections, and more. These simulations help assess the system's ability to withstand and mitigate these attacks effectively.

The dynamic testing process evaluates the time taken by the AI and blockchain-based security measures to detect and respond to security incidents. A quick response time iscrucial to minimize the impact of security breaches.

In dynamic testing, threat intelligence feeds can be included into AI algorithms to improve the system's capacity to identify new and emerging risks.

Penetration testing, or ethical hacking, is an essential part of dynamic testing. It involves authorized security experts attempting to exploit vulnerabilities in the system to assessits overall security posture.

Dynamic testing is an iterative process. The insights gained from ongoing testing are used to improve the AI algorithms, blockchain protocols, and overall security infrastructure continuously.

In order to secure data security and privacy, dynamic testing also includes assessing ifthe system conforms with pertinent security standards and laws.

7.2 TESTING APPROACHES

7.2.1 WHITE BOX TESTING

White Box Testing, recognized under multiple designations including Glass Box, Clear Box, and Structural Testing, is predicated on the internal code structure of the application. It harnesses an internal viewpoint of the system and capitalizes on programming expertise to devise test cases, predominantly performed at the unit level.

7.2.2 BLACK BOX TESTING

Black Box Testing, alternatively known as Behavioral/Specification-Based/Input-OutputTesting, refers to a software testing approach where the assessment of the software's functionality is conducted without delving into the internal code structure.

7.2.3 GREY BOX TESTING

The amalgamation of White Box and Black Box Testing results in the emergence of the grey box approach. Testers conducting this form of testing must possess authorization to peruse the design documents, which in turn facilitates the development of superior test cases throughout the entire process.

7.3 TESTING LEVELS

7.3.1 UNIT TESTING

The purpose of Unit Testing is to verify the correct functioning of individual modules within the source code. This entails the thorough examination of each unit of the application in isolation by the developer, within their own development environment. This type of testing is also known as Module Testing or Component Testing.

UNIT TESTING FOR SECURING DATA OVER NETWORK USING BLOCKCHAIN AND AI

Unit tests should concentrate on testing distinct components. For instance, you might wish to test the components that handle data encryption and decryption separately if you're developing a blockchain-based data storage system.

To make sure the system can manage unforeseen circumstances, edge case testing is essential for security-related systems. Test, for instance, what happens if the system isgiven the wrong key to decrypt data or if it is given corrupt data?

You should have unit tests for blockchain-specific features like initiating transactions, mining blocks, and confirming the integrity of the blockchain if your system relies on it for data integrity and immutability.

Test the AI algorithms in your system, if it has any, to make sure they yield reliable outcomes. Check whether the AI can recognize dangers, detect anomalies, or encrypt data.

Data for the test should be prepared with known outcomes. This enables you to contrastthe unit's actual output with what was anticipated.

For continuous integration and continuous deployment (CI/CD) pipelines, automated unit tests are essential. Make use of testing frameworks that let you run tests automatically whenever the source is modified.

You might have external dependencies in blockchain- and AI-based systems, such as blockchain networks or AI service providers. To imitate these dependencies during testing and maintain test isolation, use mock objects or stubs.

While performance and security testing should be a part of your overall testing approach, unit testing is primarily concerned with individual components. These tests can be carried out alone or as a part of system and integration tests.

Regression testing should be done when new additions or changes are made to ensure that existing functionalities, including data security measures, are maintained.

Keep thorough records of all test cases, the intended outcomes, and the actual results. This documentation helps in locating and resolving problems that were discovered during testing.

7.3.2 INTEGRATION TESTING

The evaluation of the interconnection or data interchange between the tested modules, commonly known as Integration Testing, is alternatively labeled as I&T Testing or String Testing. This phase of testing is classified into distinct methodologies, namely the Top-Down Approach, Bottom-Up Approach, and Sandwich Approach, incorporating aspects from both Top-Down and Bottom-Up techniques.

INTEGRATION TESTING FOR SECURING DATA OVER NETWORK USINGBLOCKCHAIN AND AI

You must first determine the many scenarios that your AI and blockchain-based data security solution is required to handle. Data encryption, access control, smart contracts, consensus methods, data validation, AI-driven anomaly detection, etc. might all be examples of these scenarios.

Make a collection of test data that depicts diverse real-world conditions, both typical and unusual. To mimic interactions between various system components, this data should be employed.

Make a dedicated test environment that as nearly resembles your production environment as you can. The blockchain network, AI algorithms, and all pertinent elements of the data security system should all be present in this context.

Using the selected cryptographic methods, ensure that data has been encrypted and decoded appropriately. Make sure that information is confidential at all times and is transmitted securely via the network.

To guarantee that only authorized users can access particular data and system functionalities, test various user roles and permissions.

Test the functionality of smart contracts thoroughly if your system depends on them.

Make that smart contracts function as intended and that their results match what is anticipated.

Test the efficacy of your blockchains consensus process in preserving data integrity and blocking unauthorized changes, if it uses one (such as Proof of Work or Proof of Stake).

Verify the AI models that are utilized for intrusion detection and anomaly detection. To evaluate the precision and dependability of the AI-driven security measures, use a variety of data sources.

To ensure smooth data flow and communication between the two technologies, test theintegration between the blockchain and AI components.

Check the system's performance under various loads to make sure it can withstand peakusage without jeopardizing security.

Conduct penetration tests and security vulnerability assessments to find and fix any potential system flaws.

Test the system's resilience to errors or assaults and make sure that data security is maintained even in the face of unforeseen circumstances.

Check to see if the system conforms with any applicable data protection laws and standards.

As new features are introduced or changes are made, keep testing and monitoring the system because integration testing is an ongoing process.

7.3.3 SYSTEM TESTING

The chosen testing approach is black box testing, specifically focusing on the comprehensive evaluation of the fully integrated application. This method, commonly referred to as end-to-end scenario testing, aims to guarantee the seamless functionality of the software across all intended target systems. The thorough examination encompasses every input within the application, ensuring

the attainment of desired outputs. Additionally,the testing 33 valuates encompasses the 33 valuateon of users' experiences with the application to further validate its performance.

SYSTEM TESTING FOR SECURING DATA OVER NETWORK USING BLOCKCHAIN AND AI

Define the scope and objectives of the testing.

Identify the functionalities and security features that need to be tested.

Determine the test environment, including the blockchain network and AI components. Set up the blockchain network with appropriate nodes and smart contracts.

Configure the AI components, including machine learning models and algorithms. Ensure integration between the blockchain and AI systems.

Test the security features of the blockchain network, such as encryption, hashing, andaccess controls.

Assess the AI system's data handling practices to prevent unauthorized access ormanipulation.

Check for vulnerabilities in the overall system and address potential risks. Ensure that data stored on the blockchain remains consistent and tamper-proof.

Validate the integrity of data processed by AI algorithms and prevent data poisoning orbias.

Test the system's ability to handle increasing data and user loads without compromisingsecurity.

Assess whether the blockchain and AI components can scale efficiently.

Evaluate the system's performance under various conditions, including data volume,transaction load, and AI processing.

Check for any bottlenecks or performance issues that may affect the security of the data. Conduct ethical hacking attempts to identify potential vulnerabilities in the system.

Fix any security flaws and retest to ensure they have been addressed effectively.

Assess the system's usability from an end-user perspective to ensure that it is intuitiveand easy to use securely.

Ensure the system complies with relevant regulations and standards for data securityand privacy.

Document, all test cases, procedures, and results, generate a comprehensive test report with findings, recommendations, and anyidentified issues.

CHAPTER-8

OUTPUT SCREENSHOTS

8.1 SCREENSHOTS

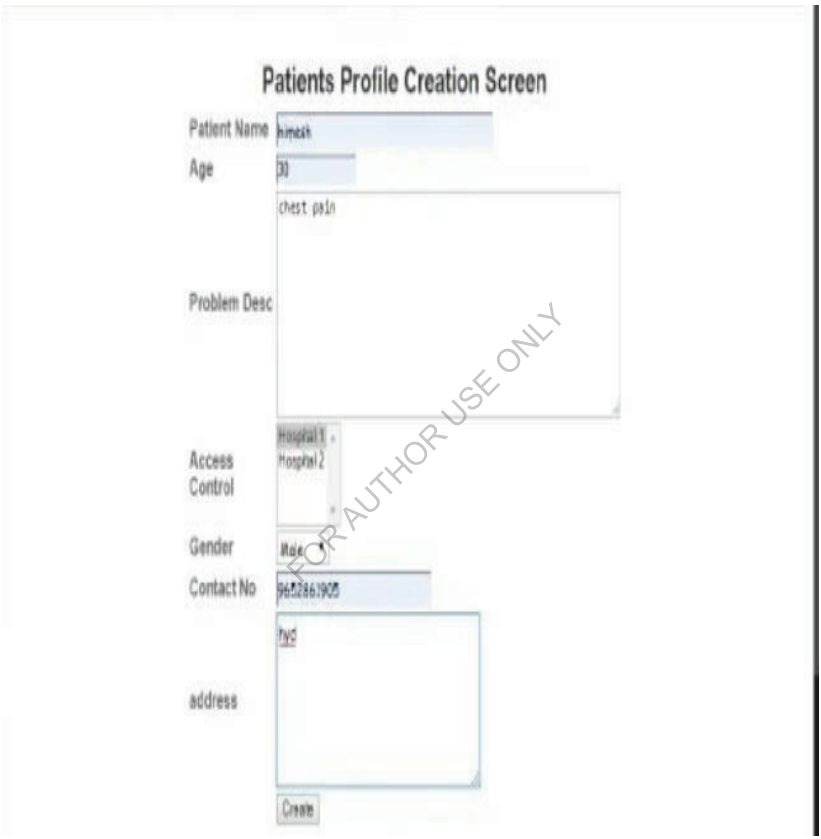

Fig 8.1 Patient Registration Page

Fig 8.2 Hospital Login Page

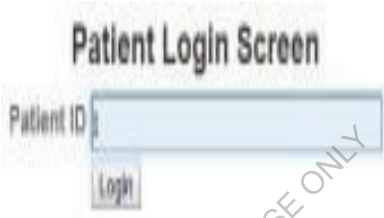

Fig 8.3 Patient Login Page

Fig 8.4 Patient Detail Page

Fig 8.5 Get Access String

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No	Address	Block Chain Hashcode
1	himesh	30	chest pain	2019-12-17	Hospital1	Male	9652861905	hyd	00f3b022952c390c39dff01d59e94ee6574a953e1fcdf18493e2

Fig 8.6 Patient Details with Hash code

CHAPTER 9

9.1 CONCLUSION

In order to address the issue of data abuse and enable trustworthy data management in an environment lacking inherent trust, we propose an innovative networking paradigm calledSec Net. Sec Net focuses on secure data storage, sharing, and computation rather than mere communication, leveraging the combined potential of AI and blockchain. Through the utilization of blockchain technologies, SecNet ensures data ownership guarantees, while also incorporating an AI-based secure computing platform and a blockchain-based incentive mechanism. These elements provide a framework and incentives for data integration and the augmentation of AI capabilities, ultimately leading to enhanced network security.

In our research, we specifically explore the application of SecNet in medical care systems, outlining typical use scenarios and presenting alternative approaches to leveraging SecNet's storage function. Additionally, we evaluate the impact of SecNet on network vulnerability in countering Distributed Denial-of-Service (DDoS) attacks, and analyze the incentive aspect of encouraging users to share security rules, thereby contributing to a moresecure network.

9.2 FUTURE SCOPE

In our forthcoming research, we intend to investigate the potential utilization of blockchaintechnology for access authorization regarding data requests. Our objective is to develop robust and comprehensive smart contracts that ensure secure data sharing and facilitate AI-based computing services within the SecNet framework. Furthermore, we aim to constructa model of SecNet and evaluate its performance extensively through a series of experiments conducted on advanced platforms. For instance, we plan to integrate IPFS [27] and Ethereum [28] to create an architecture similar to SecNet, which will serve as the basis forour analysis.

REFERENCES

[1] H. Yin, D. Guo, K.Wang, Z. Jiang, Y. Lyu, and J. Xing, ``Hyperconnected network: A decentralized trusted computing and networking paradigm," IEEE Netw., vol. 32, no. 1, pp. 112117, Jan./Feb. 2018.

[2] K. Fan, W. Jiang, H. Li, and Y. Yang, ``Lightweight RFID protocol for medical privacy protection in IoT," IEEE Trans Ind. Informat., vol. 14, no. 4, pp. 16561665, Apr. 2018.

[3] T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ``Amber: Decoupling user data from Web applications," in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 16.

[4] M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang, and S. Sen, ``Enhancing selectivity in bigdata," IEEE Security Privacy, vol. 16, no. 1, pp. 3442, Jan./Feb. 2018.

[5] Y.-A. de Montjoye, E. Shmueli, S. S.Wang, and A. S. Pentland, ``openPDS: Protecting the privacy of metadata through SafeAnswers," PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790.

[6] C. Perera, R. Ranjan, and L.Wang, ``End-to-end privacy for open big data markets,"IEEE Cloud Comput., vol. 2, no. 4, pp. 4453, Apr. 2015.

[7] X. Zheng, Z. Cai, and Y. Li, ``Data linkage in smart Internet of Things systems: A considerationfrom a privacy perspective," IEEE Commun. Mag., vol. 56, no. 9, pp. 5561, Sep. 2018.

[8] Q. Lu and X. Xu, ``Adaptable blockchain-based systems: A case study for product traceability,"IEEE Softw., vol. 34, no. 6, pp. 2127, Nov./Dec. 2017.

[9] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ``Deep learning based inference of private information using embedded sensors in smart devices" IEEE Netw. Mag., vol. 32,no. 4, pp. 814,Jul./Aug. 2018.

[10]. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ``MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 1475714767, 2017.

[11]. D. E. O'Leary, ``Articial intelligence and big data," IEEE Intell. Syst., vol. 28, no. 2,pp. 9699,Mar. 2013.

[12]. A. Halevy, P. Norvig, and F. Pereira, ``The unreasonable effectiveness of data," IEEE Intell.Syst., vol. 24, no. 2, pp. 812, Mar. 2009.

[13]. Z. Cai and X. Zheng, ``A private and efcient mechanism for data upload- ing in smart cyber- physical systems," IEEE Trans. Netw. Sci. Eng., to be published. doi:10.1109/TNSE.2018.2830307.

[14]. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, ``BlockChain: A dis- tributed solution to automotive security and privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119125, Dec. 2017.

[15]. J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ``A blockchain based privacy- preservingincentive mechanism in crowdsensing applications," IEEE Access, vol. 6, pp. 1754517556, 2018.

[16]. C. Sun, A. Shrivastava, S. Singh, and A. Gupta, ``Revisiting unreasonable effectiveness of data in deep learning era," in Proc. IEEE Int. Conf. Comput. Vis. (ICCV),Oct. 2017, pp. 843852.

[17]. W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ``When intrusion detection meets blockchain technology: A review," IEEE Access, vol. 6, pp. 1017910188,2018.

[18]. J.-H. Lee, ``BIDaaS: Blockchain based ID as a service," IEEE Access, vol. 6, pp. 22742278,2017.

[19]. K. Wang, H. Yin, W. Quan, and G. Min, ``Enabling collaborative edge computing for software dened vehicular networks," IEEE Netw., vol. 32, no. 5, pp. 112117, Sep./Oct. 2018.

[20]. A. B. Kurtulmus and K. Daniel, ``Trustless machine learning con- tracts; evaluating and exchanging machine learning models on the ethereum blockchain," 2018, arXiv:1802.10185. [Online]. Available:

https://arxiv.org/abs/1802.10185

[21]. A. L. Buczak and E. Guven, ``A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 11531176, 2nd Quart., 2016.

[22]. I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A.Courville, and Y. Bengio, ``Generative adversarial net- works," 2014, arXiv:1406.2661. [Online]. Available: https://arxiv.org/ abs/1406.2661

[23]. E. C. Ferrer, ``The blockchain: A new framework for robotic swarm systems," 2017,arXiv:1608.00695. [Online]. Available: https://arxiv.org/ abs/1608.00695

[24]. IPFS. Accessed: Jun. 5, 2019. [Online]. Available: https://ipfs.io/org

[25]. S. T. Zargar, J. Joshi, and D. Tipper, ``A survey of defense mechanisms against distributed denial of service (DDoS) ooding attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 20462069, 4th Quart., 2013.

[26]. A. Praseed and P. S. Thilagam, ``DDoS attacks at the application layer: Challenges and research perspectives for safeguardingWeb applications," IEEE Commun. Surveys Tuts., vol. 21,no. 1, pp. 661685, 1st Quart., 2019.

[27]. J. Benet, ``IPFSContent addressed, Versioned, P2P le system," 2014, arXiv:1407.3561. [Online]. Available: https://arxiv.org/abs/1407.3561

[28]. G. Wood, ``Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2018. Accessed: Jun. 5, 2019. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pd.