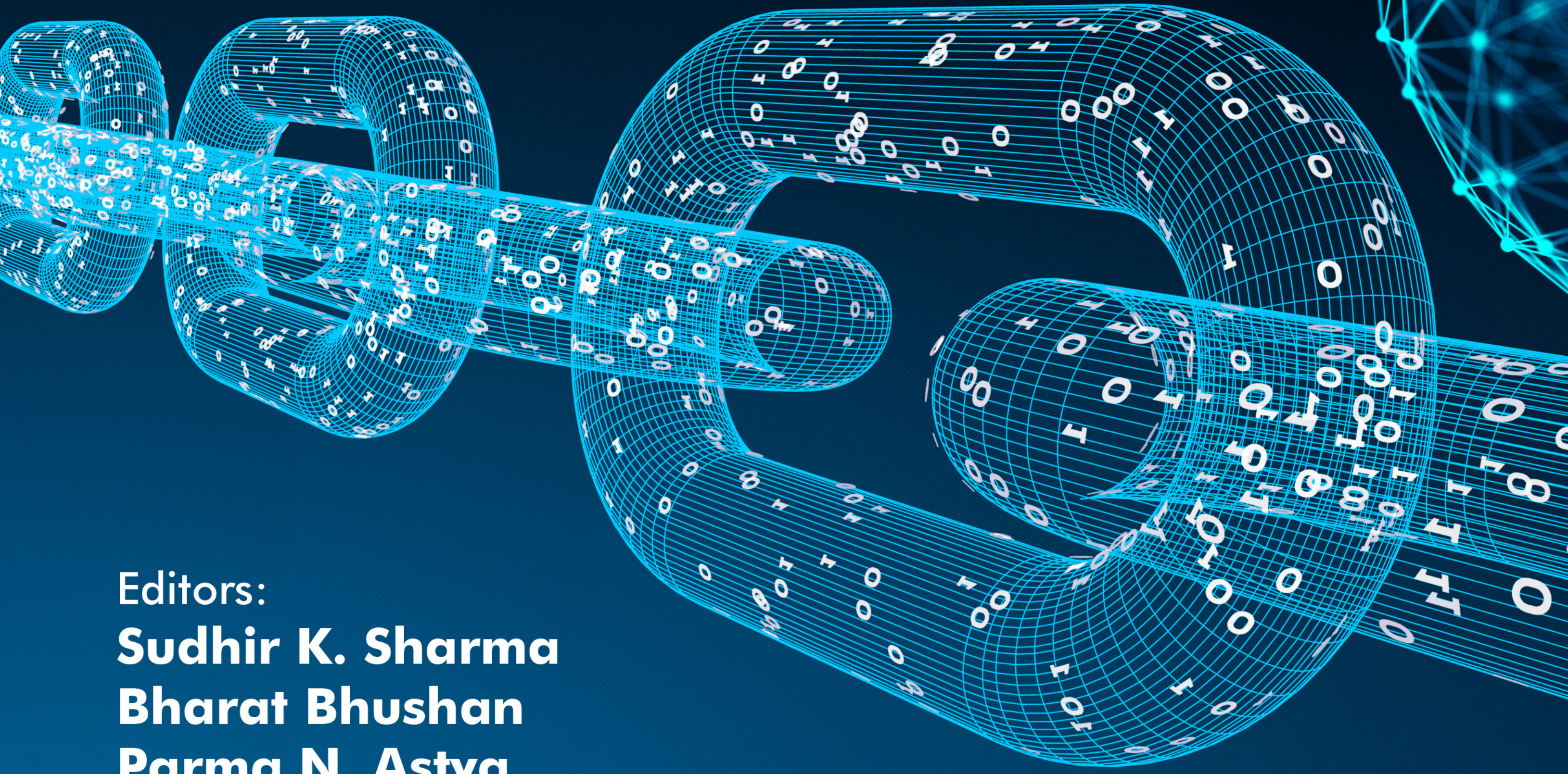
BLOCKCHAIN APPLICATIONS FOR SECURE IoT FRAMEWORKS:

TECHNOLOGIES SHAPING THE FUTURE



Editors:

Sudhir K. Sharma
Bharat Bhushan
Parma N. Astya
Narayan C. Debnath

Bentham Books

Advances in Computing Communications and Informatics

(Volume 1)

Blockchain Applications for Secure IoT Frameworks: Technologies Shaping the Future

Edited by

Sudhir K. Sharma

Institute of Information Technology and Management
D-29, Institutional Area
Janakpuri
New Delhi
India

Bharat Bhushan & Parma N. Astya

School of Engineering Technology
Sharda University
Uttar Pradesh 201310
India

&

Narayan C. Debnath

School of Computing and Information Technology
Eastern International University
Bình Dương
Vietnam

Advances in Computing Communications and Informatics

Volume # 1

Blockchain Applications for Secure IoT Frameworks: Technologies Shaping the Future

Series Editors: Pradeep Kumar Singh, Bharat Bhargava & Wei-Chiang Hong

Volume Editors: Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath

ISSN (Online): 2737-5730

ISSN (Print): 2737-5722

ISBN (Online): 978-1-68108-862-4

ISBN (Print): 978-1-68108-863-1

ISBN (Paperback): 978-1-68108-864-8

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Ltd.
Executive Suite Y - 2
PO Box 7917, Saif Zone
Sharjah, U.A.E.
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

The Internet of Things (IoT) is an emerging technology that has enabled connection and communication between both virtual and physical objects, thereby improving our quality of life. The definition of IoT has evolved because of the convergence of numerous technologies such as embedded systems, commodity sensors, machine learning, and real-time analytics. IoT contributes towards the concept of connected vehicles, connected health, wearable technology, home automation, and appliances having remote monitoring capabilities. Even though these systems provide numerous advantages, the current centralized architecture brings forth numerous issues related to privacy, security, transparency, data integrity, and single point of failure. This, in turn, inhibits the future development of these IoT-based applications. Further, the radical digitization of industry coupled with the explosion of the Internet of Things (IoT) has set up a paradigm shift for industrial and manufacturing companies. Owing to these issues, it becomes necessary to integrate IoT with a distributed ledger technology. Blockchain technology, an immutable, shared, distributed ledger, is the most suitable choice for a variety of reasons. It stores the various transaction information in a peer-to-peer (P2P) network and promotes information sharing among the network users. Owing to the fault tolerance capabilities, decentralized architecture and cryptographic security benefits such as authentication, data integrity, pseudonymous identities, security analysts and researchers consider blockchain to resolve privacy and security issues of IoT. The use of hash functions, timestamps, and sophisticated cryptographic algorithms in blockchain technology enables a secure computing environment and provides a tamper-proof ledger that can safeguard against possible attacks. Also, blockchain is used in numerous applications such as healthcare, intelligent transportation, supply chain management, identity management, voting, and maintaining government records. Due to these reasons, blockchain is considered the most disruptive and emerging future technology that will provide numerous opportunities to various industries. The emerging and promising state-of-the-art IoT and blockchain technology motivated us to propose this book, focusing on various aspects of IoT and blockchain systems like trust management, identity management, security threats, and access control and privacy. The book provides a comprehensive discussion on integrating the IoT system with blockchain technology, highlights the benefits of integration, and how blockchain technology resolves the issues of IoT systems.

Sudhir K. Sharma
Institute of Information Technology and Management
D-29, Institutional Area, Janakpuri
New Delhi
India

List of Contributors

Aashna Jha	Department of Electronics and Communication, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India
Ana Carolina Borges Monteiro	School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo , Brazil
Arepalli Peda Gopi	Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India
Bharat Bhushan	School of Engineering and Technology, Sharda University, Greater Noida, India
C. Priya	Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
Deepak Kumar Sharma	Department of Information Technology, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India
Deepti Gupta	Amity School of Engineering and Technology, Amity University, Noida, U.P., India
H Abhijith	Amity School of Engineering and Technology, Amity University, Noida, U.P., India
Ila Kaushik	Krishna Institute of Engineering & Technology, Ghaziabad, U.P, India
Jawed Ahmed	Department of Bioengineering, University of California, Riverside, CA, USA
J. S. Shyam Mohan	Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India
K. Sheela	Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
Khwaja M. Rafi	Director, Mewat Engineering College, Palla, Distt. Nuh, HaryanaIndia,
Mohd. M. Haque	School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India
Mohammad Maksuf Ul Haque	Department of Computer Science, Jamia Millia Islamia, New Delhi, India
Mohammad Sufian Badar	Department of Bioengineering, University of California, Riverside CA, USA
Nagendra Panini Challa	Department of Information Technology, Sri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh 534202, India
Nikhil Sharma	HMR Institute of Technology & Management, Delhi, India
Nuggu Kowshiki	Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India
Pasumarthy Swathi	Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India
Rangel Arthur	Faculty of Technology (FT), State University of Campinas (UNICAMP), Limeira, São Paulo, Brazil

Reinaldo Padilha França	School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo , Brazil
R.S.M. Lakshmi Patibandla	Department of IT, Vignan's Foundation for Science, Technology and Research, Andhra Pradesh, India
Saakshi Bhargava	Department of Physical Sciences and Engineering, Banasthali Vidyapith, Tonk, Rajasthan, India
Shazmeen Shamsi	Department of Computer Science, Jamia Millia Islamia, New Delhi, India
Shilpi Sharma	Amity School of Engineering and Technology, Amity University, Noida, U.P., India
Shweta Paliwal	Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology (MIET), Meerut, India
Somya Goyal	Manipal University Jaipur, Jaipur, India Rajasthan and Guru Jambheshwar University of Science and Technology, Hisar, India
Sudhir Kumar Sharma	Institute of Information Technology and Management, Janakpuri, New Delhi, India
Sukriti Goyal	HMR Institute of Technology & Management, Delhi, India
Sushil Kumar	Department of Computer Science, Jamia Hamdard University, New Delhi, India
Vejendla Lakshman Narayana	Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India
Vishakha	HMR Institute of Technology & Management, Delhi, India
Yuzo Iano	School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo , Brazil

CHAPTER 1

An Overview of Smart Grid in the Current Age

Reinaldo Padilha França[1,*], **Ana Carolina Borges Monteiro**[1,*], **Rangel Arthur**[2] and **Yuzo Iano**[1]

[1] *School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil*

[2] *Faculty of Technology (FT), State University of Campinas (UNICAMP), Limeira, São Paulo, Brazil*

Abstract: Smart Grid is defined as an intelligent electrical distribution system that offers bi-directional energy, which flows from producers to consumers, intending to optimize use to reduce costs and improve the performance of the electricity network, which requires a balance between generators, operators, and system distributors, providing benefits , including reduced power losses, lower costs, and better measurement of consumption with better control, enabling a reduction in carbon emissions. With sensors installed in the electrical networks sending data related to energy consumption directly from the consumer unit, they enable more effective and efficient network planning. Besides, the network is designed to reduce the occurrence and duration of power outages as much as possible. In it, electromechanical consumption meters are replaced by digital smart meters, representing a true revolution in energy supply, meaning that the Smart Grid is a system that automates not only the monitoring but the entire management of electricity use. This chapter contributes to the discussion and overview of Smart Grids, their applications in the current era, as well as categorizing and synthesizing the technology's potential.

Keywords: Bi-directional energy, Data analysis, Intelligent electrical, IoT, Sensors, Smart architecture, Smart cities, Smart grid.

1. INTRODUCTION

The search for sustainability-related to digital transformation has created new possibilities for the world, with actions aimed at reducing environmental damage with a greater objective than simply saving, but it is necessary to make intelligent and conscious use of what is at disposal.

[*] **Corresponding authors Reinaldo Padilha França and Ana Carolina Borges Monteiro:** School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil and School of Electrical Engineering and Computing (FEEC), State University of Campinas (UNICAMP), Campinas, São Paulo, Brazil; E-mails: padilha@decom.fee.unicamp.br and monteiro@decom.fee.unicamp.br

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

Energy management is a prerequisite for a sustainable environment, and Smart Grids are an essential pillar for its achievement. The spread of renewable energy sources has led to a profound modernization of traditional electricity distribution systems and how they are effectively distributed. Smart Grid is defined as an intelligent electrical distribution system that delivers bi-directional energy flows from producers to consumers. Unlike traditional power grids, where power is generated by only one plant and distributed to end customers through the large transformer and substation networks, in Smart Grid, end customers also act as producers [1, 2].

Internet of Things technology is enabling cities around the world to implement a series of digital transformation projects, such as reducing car traffic in major cities and energy consumption. In addition to its use in home life, IoT promises to revolutionize industries, the security market, and even the medical field. Electricity consumption was also largely impacted by technology. Efforts are being made to design and implement energy-efficient networks that use Smart Grid parameters and apply the Internet of Things, making it possible for the network to work in less time and reduce power consumption [3].

A company's entire infrastructure depends on electricity, which requires continuous management of its use. In parallel with the search for sustainability, digital transformation has also added to the creation of new possibilities for managing this resource. The concept of this trend refers to a new power distribution architecture that can automate all management of electricity use. For the Smart Grid to function, it is necessary to switch analog meters to digital meters. These are safer, and especially intelligent, devices that enable the integration of information between other connected users [4].

Smart Grid is generic for applying computational intelligence and networking skills to an electricity distribution system. In recent times, this concept has gained a lot of prominences , especially in Smart Grid projects that seek to improve operations, maintenance, and planning, ensuring that each component of the power grid can “talk” and “listen.”It is, therefore, a highly automated, efficient, self-healing, a bi-directional pathway of energy, enabling i nterconnected communications for a highly reliable and efficient utopian world of energy production and distribution [5].

Considering that in many places, a power company will only know that service is disrupted if a customer calls in a Smart Grid scenario, the company will immediately know why certain network components, such as the use of smart meters in the affected area, have stopped to send sensor data. By ensuring that all network components, from transformers and power lines to household, commercial and industrial electrical meters, have IP addresses and are capable of using bidirectional communication, the company can manage distribution more efficiently. Also, it needs to be proactive in maintenance and respond to outages faster. So, another important component of Smart Grid technology is automation [6].

Basically, it must communicate in an integrated automated way between components of the power grid, employ detection and measurement technologies, automated controls for distribution and repairs, better dashboard management, and decision support software. It is correct to say that a Smart Grid is an example of the Internet of Things (IoT), in which almost any object can be equipped with a unique identifier and given the ability to communicate over the web [7].

A Smart Grid is equipped with sensors that collect and transmit data since this information transmission allows to automatically adjust the electricity flows. Remotely located controllers are then informed of the situation in real-time and can act immediately if there is a problem occurring virtually without human intervention. Besides, this type of grid can communicate with any smart meter , for example, turn on consumer appliances automatically when there is too much electricity on the grid, and its prices are therefore lower [8].

One of Smart Grid's biggest advantages is the ability to track energy performance in real-time. Unlike the traditional meter, where consumption data is collected once a month, digital allows constant tracking. In this way, irregularities are quickly identified and predictive, preventive, and corrective actions can be taken to avoid waste and set goals to improve the company's energy consumption. Also, a more sustainable business model is established, as it enables the reduction of carbon dioxide emissions and other pollutant residues [9].

Smart Grid is a promise of a flexible, resilient, performance-safe power grid that allows network resources to be exploited in real-time to optimize productivity. Characterized by the deployment of many thousands of intelligent and interactive control devices, sensors and meters, it ensures the correct interaction between all these elements, as well as significantly improving the network's efficiency, reliability, and freedom for the end customer to control. their consumption conditions [10].

Among leading distribution automation and distributed power resource applications, this model can provide intelligent energy storage and provide real-time response to fluctuating demand. All this plus client-side demand management from a two-way conversation between devices on the network and also intelligent consumer devices on the edge of the user. In addition to placing the customer "in control" of their own energy use, this ploy ensures highly

CHAPTER 2

Dynamic Strategies of Machine Learning for Extenuation of Security Breaches in Wireless Sensor Networks

Shweta Paliwal[1,*]

[1] *Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology (MIET), Meerut, India*

Abstract: Wireless sensor networks (WSNs) have turned up as a promising technology due to their deployment nature and the knock-off feature of cost-effectiveness. The rapid increase in the demand for wireless applications has opened up new security vulnerabilities which are related to their infrastructure-less nature and their nature of transmission and hence made WSNs the centre point of attraction for attackers and intruders. Machine Learning has embedded comprehensive solutions to accord with modern security breaches. It has gained a mark of deterrent technology by shoring up the infrastructure of security through mapping security breaches and performing the identification of unknown patterns. This chapter focuses on the illustration of security breaches in wireless sensor networks along with the glimpse of reduction in attacks through dynamic algorithms and strategies of Machine Learning. We have proposed some feature selection methodologies in order to identify the best features out of the available network dataset. These feature selection methods are evaluated against the existing machine learning classifiers in order to identify the best feature selection strategy and the best classifier.

Keywords: Cyber security, Feature selection, Machine learning, Wireless Sensor Networks (WSNs).

1. INTRODUCTION

The tremendous growth in the field of Information Technology and Communication has paved the way for the evolution of Wireless Sensor Networks (WSNs). Today wireless sensor networks have marked their presence in various application areas of medicine, military, smart spaces, and many others. A wireless sensor network (WSN) is defined as a collection of spatially dispersed network devices along with dedicated sensors to monitor and record the physical condition

[*] **Corresponding author Shweta Paliwal:** Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology (MIET), Meerut, India; E-mail: shwtplwl23@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

of the environment. Wireless sensor networks can either be demand-driven or event-driven. In event-driven sensor networks, the network triggers as soon as it senses changes in the monitored area, whereas, in demand-driven, the network serves as an updated database for a client. Wireless sensor networks are comprised of several tiny sensor nodes that are deployed either randomly or deterministically [1]. These nodes gather the data from the environment and transmit the sensed data to the base stations for further processing. WSNs provide cross-layer design and scalability along with the capacity to handle the failure of nodes. Different types of sensors such as seismic, magnetic, visual, *etc*. are embedded within the WSNs, thereby monitoring ambient situations.

The characterization of sensor nodes depends on their storage capacity, limited processing power, and limited energy. Based on the nature of nodes, wireless sensor networks are classified into two types of networks, namely homogeneous and heterogeneous sensor networks. A network where all sensor nodes have a similar property for communication, memory, energy, and reliability is termed a homogeneous network [2]. Due to the nature of transmission of wireless networks, security has become a critical issue. Not only security but the designers of wireless sensor networks must also focus on the issues related to the reliability of data, aggregation of data, and fault detection. Since the sensor nodes are capable of operating both in ad hoc networks as well as the normal networks, security goals could be categorized into two types; Primary Security Goals and Secondary Security Goals.

Machine learning provides low complexity estimation for the model of the system, thereby being deployed in a complex environment of the wireless sensor networks. Designers of wireless sensor networks are focusing on machine learning algorithms to gain new insights and knowledge about the unreachable location. It can be seen that wireless sensor networks are adopting machine learning to increase the security of the communication channel as machine learning is capable of dealing with the dynamic behavior of the wireless sensor networks.

The paper has identified different feature selection methodologies from the network dataset. Feature selection methodologies are important as they fasten up the training of the ML model and at the same time reduce the complexity of the model, thus providing easier interpretation. We have identified the best feature selection strategy and then evaluated it against several machine learning classifiers to identify the algorithm with optimized performance in the detection of security breaches.

Section 2 describes the security concerns in WSNS followed by a description of Machine learning in Section 3. Section 4 describes how ML addressed different security issues, and Section 5 describes the approaches that have been developed to combat these issues. The proposed methodology has been described in Section 6. Section 7 describes the conclusion of the entire work.

2. SECURITY CONCERNS IN WIRELESS SENSOR NETWORKS

Evolution in the field of manufacturing industries and wireless communication networks has contributed to the growth of WSNs. They are made up of cost-effective sensor nodes that release a high amount of energy. Several characteristics make WSNs prone to security attack which includes resource-constrained nature of sensor nodes and ad hoc deployment of nodes. The basic requirement for WSNs to survive includes reliability, availability, and energy efficiency. Denial of service attacks and eavesdropping attacks targets the confidentiality and integrity of the data being transmitted over the network, and Flooding and Jamming attacks are related to the power consumption of the network [3-4]. Hence it can be stated that there are several security attacks that target the sensitive points of WSNs, such as Bandwidth, Power, and Routing Mechanism of WSNs, thus opening up new gateways for intruders. WSNs are more vulnerable to Man in the Middle-Security Attack as they provide complete control over information that is transmitted over the network. The attackers target the confidentiality and integrity of data.

2.1. Eavesdropping Attack

Eavesdropping attack forms the base for other attacks and is a serious security threat to wireless sensor networks. There are two sorts of eavesdropping attacks in wireless sensor networks; passive eavesdropping, where the information is detected by malicious nodes through the listening of message transmission in a wireless broadcasting medium. Active eavesdropping, where information is captured by malicious nodes disguising themselves to be authorized nodes through queries sent to the transmitter.

2.2. Jamming Attack

Jamming is considered as a special class of DOS (Denial of service) attack. In a Jamming attack, high-frequency radio signals are emitted that disrupt the operations of the transmitter. A jammer could either be a simple transmitter or an entire jamming station equipped with special equipment.

CHAPTER 3

IoT- Fundamentals and Challenges

Mohammad Maksuf Ul Haque[1], **Shazmeen Shamsi**[1], **Khwaja M. Rafi**[2] and **Mohammad Sufian Badar**[3,4,*]

[1] *Department of Computer Science, Jamia Millia Islamia, New Delhi, India*

[2] *Director, Mewat Engineering College, Palla, Distt. Nuh, Haryana, India*

[3] *Department of Bioengineering, University of California, Riverside, CA, USA*

[4] *Salfia Paramedical Institute Darbhanga, SPI Darbhanga, Bihar 846001, India*

Abstract: The Internet of Things (IoT) is a revolutionary technology that aims at embedding everything we interact with or use with the capability to share and receive information over the internet. By everything, we mean all plausible things, from the refrigerator in your kitchen and washing machine to a soil moisture sensor on a farm and sprinklers in a stadium field. It has limitless applications in every field, including medical, industrial/manufacturing, security, *etc.*, to name a few. This myriad of applications makes IoT a difficult concept to comprehend. To tackle this issue, we present this work which aims at defining the loosely bounded concept of IoT comprehensively with related examples and lesser technical jargon than usual. Slowly, we will dwell into technical aspects and real-life applications by talking about Wireless Sensory Networks (WSNs, a subset of IoT), Distributed Ledger Technology (or Blockchain), another revolutionary technology that is merging with IoT to give rise to an even more secure and robust range of applications. Then, we will discuss the third pillar, Artificial Intelligence (AI), that, when paired with the aforementioned systems, breathes life into the devices we interact with daily. Finally, we will weigh the challenges and prospects of the field.

Keywords: AI, Artificial Intelligence, Blockchain, Distributed Ledger Technology, IoT architecture, Internet of Things, IoT, IoT security, Machine Learning, ML.

1. INTRODUCTION

The chapter aims at explaining the fundamental concepts of the “Internet of Things” abbreviated as **IoT**. We humans, as intelligent beings, have always strived to make our lives easier, from the simplest things like a pressure cooker to state of the art self driving cars [1] and UAVs used by the military for

[*] **Corresponding author Mohammad Sufian Badar:** Department of Bioengineering, University of California, Riverside, CA, USA; Tel: +1318 2783 121; E-mails: msbadar@engr.ucr.edu, director_academic@salfiainstitute.edu.in

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

surveillance [2], *etc.* IoT is yet another technological paradigm that is working towards making our lives easier and enriching our experiences and interactions with the things around us. The concept of IoT is a little difficult to grasp because of the diversity of things involved and the plethora of current and possible applications. Wikipedia defines IoT as *"The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."* [3]. While one can make some sense out of what it means, it is somewhat technical. The definition given by McKinsey, though small, seems more logical and makes the concept a little more understandable, "*Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet"* [4].

As mentioned earlier, the definitions in and of themselves are acceptable, yet they fall short of encompassing the depth and breadth of the concept. In this chapter, we will learn the fundamentals through various examples of what IoT is, but for now, let us talk about the other revolutionary technologies that go hand in hand with IoT to give us that enhanced interaction with devices around us. Artificial intelligence, abbreviated as "AI", is a field of computer science and engineering that makes machines intelligent or, to be more precise, intelligent computer programs [5]. AI-enabled devices can by themselves automatically perform tasks that generally require human assistance or intervention. The definition given by Andrew Moore defines AI simply and concisely as, "*Artificial intelligence is the science and engineering of making computers behave in ways that, until recently, we thought required human intelligence*."

This intelligence is achieved mostly through Machine Learning or ML and enables programs and software to learn and attain or mimic human-like intelligence, *i.e.*, become Artificially Intelligent. One can say that ML is how computers learn to become intelligent or as Tom M. Mitchell said, "*Machine learning is the study of computer algorithms that allow computer programs to automatically improve through experience*."

Next is another Technology whose popularity has erupted in recent years, the Distributed Ledger Technology, more popularly known as Blockchain, which is a way of maintaining records. Technically, Blockchain is a distributed, decentralized, public ledger [6]. At its most basic level, blockchain is just a chain of blocks, but not in the traditional sense of those words. When we say the words "block" and "chain" in this context, we are talking about digital information (the "block") stored in public databases linked together (the "chain"). Both of these technologies, *i.e.*, AI and Blockchain are paving the way for more powerful, beneficial, and secure IoTsystems [7, 8].

The chapter discusses the history of IoT and then goes on to describe what IoT means through various examples and scenarios. After clearing the vast and vague concept of IoT, it talks about the fundamental principles, architecture, and frameworks of the technology. From there, it explores the current challenges in this field like scalability and security [9] and what can be done about it. In the end, this chapter leaves the reader with hints of what and where the future of IoT might be.

The chapter aims at developing a clear understanding of IoT. It provides the reader with a perspective regarding the emergence of IoT, how it came to be what it is now, and then it talks about IoT as in the real world around us, so that the omnipresence of these devices embedded with the internet can be understood more clearly. By discussing the fundamentals, architecture, *etc.*, it familiarizes the reader with the technicalities involved in IoT and the requirements and considerations to be paid attention to while developing an IoT solution. It then enriches the reader with the current challenges of the field to give an understanding of what we lack in. At last, with prospects about the expansion of IoT, we have to give the reader something to think about and work on if they want to pursue a career in the field of IoT.

2. HISTORY OF IOT

In the world of technology, one would consider the IoT as something old. The thought or vision of machines communicating with one another can be found in the works of people like Nikola Tesla's interview with Colliers in 1926 [10] and literature from the early 1800s. In a way, machines can be said to be in contact since the first Telegraph in the mid-1800s. In 1900, the first Voice over Radio transmission (Wireless telegraphy), and many more inventions and innovations in the field of communication and electronics followed, laying the foundation for IoT. Amidst all the rapid advancements, the development of computers began in the 1950s.

The Internet, a significant component of the IoT, started as part of a military defense project called DARPA in 1962 and evolved into the ARPANET in 1969. Commercial service providers started supporting the public use of ARPANET around the 1980s, which allowed the modern Internet to come into existence. Internet and communication technologies were quintessential for IoT's development. IPV6's decision to increase address space was another important component in developing a functional IoT.

CHAPTER 4

IoT Based Energy Conservation of A Smart Home

Somya Goyal[1,*] and **Sudhir K. Sharma**[2]

[1] *Manipal University Jaipur, Jaipur, Rajasthan and Guru Jambheshwar University of Science and Technology, Hisar, India*

[2] *Institute of Information Technology and Management, Janakpuri, New Delhi, India*

Abstract: Smart home is one of the most attractive application of Industry 4.0. This work proposes a smart system to conserve energy in smart home implementation using wireless sensor networks (WSNs). The proposed work is aimed to lessen the immaterial consumption of electricity in a smart home. The home is supplied with Arduino, sensors, and connected WSN. The model observes the movement within the house premises and controls the power cutoff decided by the control center connected *via* WSNs. To detect the motion, passive infrared (PIR) sensors are deployed. As the PIR sensor detects the motion into the room, the lights are automatically turned on and then, if no motion is observed after a threshold time, the lights are automatically switched off. In this manner, the wastage of electricity can be controlled. Experimental results show that the consumption of power can be decreased by at the rate of 40% with the proposed model in comparison to the situation in absence of any such smart control. The validation of proposed model shows that the proposed system is feasible, effective, and not so expensive to implement.

Keywords: Energy conservation, Passive infrared sensor (PIR), Smart homes, Wireless sensor networks (WSNs).

1. INTRODUCTION

A smart home is a term utilized for a home that is outfitted with electrical and electronic gadgets being worked on utilizing distant regulators (smartphones and so on). It utilizes some innovation for checking the atmosphere by means of introducing different sensors in the premises and afterward control the electronic gadgets from the external world. The keen home has additionally alluded as a home robotization framework. It is discovered to be exceptionally successful for rationing energy and can be easily introduced in structures. Considering multifold advantages of remote innovation over wired one, the smart home idea depends on

[*] **Corresponding author Somya Goyal:** Manipal University Jaipur, Jaipur, Rajasthan and Guru Jambheshwar University of Science and Technology, Hisar, India; Tel: +91-8168361767; E-mail: somyagoyal1988@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

the WSN. The attraction for home mechanization frameworks in homes and workplaces is consistently expanding. A smart home or computerized home is an extraordinary arrangement in a house in which the electronic gadgets are controlled remotely or automatically with the help of internet connectivity of the gadgets, exceptionally agreeable premise with the arrangement of offices to distantly control the types of gear along with the capacity of gadgets to get balanced without anyone else to explicit circumstances, as appeared in Fig. (**1**).

Fig. (1). Smart Home-Controlling all appliances with a single interface.

In 2013, the value of the market business for home automation was approximately US$5.77 billion, and in 2020, it reaches US$12.81 billion [1]. The composition of smart home systems is as follows:

i) Input the readings from the environment *via* sensors – smoke sensors, moisture sensor, temperature sensors, ii) Constant observation and input from the sensor for fire detection, CCTV footage analysis, iii) Automated controlling feature – automated control of lights, fan, A/C, automated water sprinklers in case of fire, fire alarms and iv) AI and Logic – smart security mechanisms.

1.1. Background

IoT is the spine for the home mechanization innovation as these IoT gadgets are basic segments of the smart home idea, which incorporates lighting, heating, and cooling, and security frameworks [2]. One of the significant advantages of such excellent usage of IoT in 'Smart Home' is the energy protection *via* consequently controlling the lights and other electronic apparatuses like turning off the supplies naturally when no one is in the room. Industry 4.0, AI, Cloud computing, and IoT enables the interconnection of devices, vehicles, instruments, allows fabrication of sensors to get readings and the data feed on the sensors is sent *via* a network to the cloud where the AI logic is executed to make smart decisions and automate the control of smart home [3]. IoT enlarged with sensors and actuators, turns into a sort of digital-physical framework, incorporating shrewd homes, keen transportation, and brilliant urban communities.

1.2. Motivation

A home mechanization framework is conveyed to control the lighting, atmosphere, and electrical/electronic machines. It additionally incorporates savvy security like controlling the entrance and disturbing. A smart home associated with the Internet changes the family into IoT gadgets.

1.3. Organization of Chapter

The chapter is composed as follows: Section 2 examines the advantages of Smart Home. Later Section 3 brings a look for energy preservation utilizing Smart Home innovation which is trailed by the conversation of the set of experiences. Section4 depicts the engineering and system for the shrewd home. At that point, Section 5 incorporates the usage with the ZIGBEE standard, and other execution alternatives are likewise talked about here. Segment 6 presents the utilization of IoT for protecting Cultural Heritage (CH). Section 7 finishes up the part with the comments for future investigation.

2. BENEFITS OF SMART HOME

The multi-overlay advantages of Smart Home innovation can be summarized as follows (appeared in Fig. (**2**)):

1. Distantly managing the absolute of your home contraptions from one spot offers comfort and having all the machines related through one interface is an astounding improvement to the degree progression and home affiliation.
2. This creation progress is correspondingly flexible for new contraptions and machines. Sharp home structures are greatly adaptable with the accommodation of new contraptions and other progress.
3. It maximizes home security. when security and surveillance features are laced in your sharp home connection, your home security can take off. Home robotization structures can interface headway finders, surveillance cameras,

CHAPTER 5

Blockchain: Concept and Emergence

Shazmeen Shamsi[1], Mohd. M. Haque[2], Sushil Kumar[3], Jawed Ahmed[4] and **Mohammad Sufian Badar[4,5,*]**

[1] Department of Computer Science, Jamia Millia Islamia, New Delhi, India

[2] School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India

[3] Department of Computer Science, Jamia Hamdard University, New Delhi, India

[4] Department of Bioengineering, University of California, Riverside, CA, USA

[5] Salfia Paramedical Institute Darbhanga, SPI Darbhanga, Bihar 846001, India

Abstract: Artificial Intelligence (AI), Machine Learning (ML), and Internet of Things (IoT) are incredible instances of the technology paradigm and have brought about revolutionary changes in the communication, internet, and digital sectors coalesced into one and induced a landslide shift in the lifestyle of mankind. But the privacy concerns of the individuals can be trustfully and transparently addressed only by the use of ingenious contemporary technology, the Blockchain. Blockchain is a kind of distributed ledger technology that uses a peer-to-peer, distributed network to make a continuous, growing chain of time-stamped records to form a digital ledger. It is decentralized, which means that it can not be controlled by a central authority. It has numerous advantages like transparency, immutability, decentralization and can be incorporated in almost any sector of the society to increase the security of the transactions being carried out. This chapter predominantly focuses on the concepts of Blockchain and aims to do a comprehensive survey on its advantages and applications and also highlights the future prospects because even though it is so popular today, this technology is still in its infancy.

Keywords: AI, Artificial Intelligence, Blockchain, Decentralization, Distributed Ledger Technology, Immutability, Internet of Things, IoT, ML, Machine learning, Transparency.

1. INTRODUCTION

"The blockchain revolution has a greater potential than anything we've seen in history. It's bigger than the Internet revolution, how it's going to restructure society."

—Patrick Byrne

[*] **Corresponding author Mohammad Sufian Badar:** Department of Bioengineering, University of California, Riverside, CA, USA; Tel: +13182783121; E-mails: msbadar@engr.ucr.edu, director_academic@salfiainstitute.edu.in

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

The above remark made by Patrick Byrne, CEO and founder of Overstock.com, is as apt as it can be. Today, Blockchain technology is taking the globe by storm. The enormous amount of buzz and hype that this technology has created is attracting the attention of a massive number of researchers and scientists and will eventually create the dawn of a new revolution. This chapter aims to provide a brief but clear understanding of the important aspects of this technology among the readers.

The ultimate objective of mankind is the absolute modernization of his lifestyle for attaining the highest levels of comfort. This can practically be achieved only with the development and evolution of science and technology, which eventually gives us a plethora of immensely useful applications that make life easy for us. We are currently living in an era where the world is changing at a rapid pace, and there is a constant shift of the common mass towards contemporary technologies. These innovations have affected every industry, be it business, healthcare, energy, financial markets, and so on, to the extent that in recent times, these technologies have reached the comfort of our homes and affected the way we live and socialize [1]. In this world powered by technology, everything comes at a cost We are living in times where we are experiencing a gradual transition from cash to cashless payments. Electronic Cash or E-Cash, the digital form of cash, is allowing easy and hassle-free transactions of money over the internet. This invention is in and of itself a commendable achievement that has caused a stir in the world of trade and commerce, and the immense importance of which can be understood during pandemics like Covid-19. But cybercrooks, with their felonious talents, are ever-ready to make some profit by breaching data of the transactions being carried out. Secure online transactions that involve third parties also cannot always be trusted. Let alone cybercriminals and private third parties, it has often been seen that the economic growth and development of most of the developing countries is often impeded by corrupt government officials who misuse their authority to satisfy their greed for monetary gains. Blockchain technology, which first came into the picture with the advent of Bitcoin in 2008 [2], promises decentralized and secure transactions over the internet and is a successful attempt to solve these problems.

Blockchain is a magical technology that can be clubbed with almost all other technologies available today to add to their benefits and make them safe and secure for use. It is a Distributed Ledger Technology that records and maintains transactions chronologically, occurring on a peer-to-peer scale where every peer essentially maintains a copy of the transactions being carried out. An important point to be noted is that ‘no third party is involved’ and validation of new blocks to be added to the chain occurs only if at least 51% of the participants vote in favor, otherwise it is rejected. Now you must be wondering, what are blocks?

They can simply be understood as pages of a record book that constantly register the latest transaction being carried out. Once a block runs out of memory (think of it as a page being filled with records), a new block is needed to be generated for which voting is done for its final validation and generation.

Blockchain is a revolutionary technology that came into practical existence with the advent of the cryptocurrency, Bitcoins, which caused a lot of excitement among the people and has intrigued researchers to study it thoroughly. Learning about it would help us remain updated with the most demanding skills of today. The true potential of this revolutionary technology needs to be understood by all so that we can make its best use. It is expected to re-shape the industrial trends and cause a transition from paper-based/non-secure online transactions to secure, privacy-preserving, immutable e-transactions.

This chapter will give you a basic idea of Blockchain Technology. Each topic is explained in a detailed but crisp manner. The authors have tried to make the chapter more interesting by incorporating a hands-on activity about the deployment of smart contracts to attract the interest in this topic of the readers. It is hoped to generate a clear understanding among the readers about this incredible technology which is way ahead of its time.

In the following chapter, we will first study how the need for this technology arose, followed by its history. We will then be introduced to the different elements that are essentially a part of every blockchain network. We will then learn about its features owing to which this technology has become immensely important in today’s world. Next, we will study the types, working, applications, advantages, and challenges related to this topic.

2. THE NEED FOR BLOCKCHAIN TECHNOLOGY

The need for this technology arose with the International Banking Crisis which led to the collapse of investment in 2008. Bitcoin cryptocurrency, which was the first practical example of this technology, brings along with it many advantages such as efficiency, cost-effectiveness, reliability, and a privacy-preserving secure system for creating and recording financial transactions. With an ever-increasing human population and urbanization, the number of transactions being carried out is increasing exponentially and is speculated to affect the complexity, efficiency, and cost of the current systems and in turn, increase its vulnerability [3]. The current digital transactions rely on trusted third parties to fulfill their objectives. Whether these parties can be trusted or not is a big question. Though these third parties which can be anyone- a Government Agency or a private owner- claim that the transactions are carried out in a secure environment, is it so? Studies have

CHAPTER 6

Industrial Revolution: Blockchain as a Wave for Industry 4.0 and IIoT

Sukriti Goyal[1], **Nikhil Sharma**[1,*], **Ila Kaushik**[2] and **Bharat Bhushan**[3]

[1] *HMR Institute of Technology & Management, Delhi, India*

[2] *Krishna Institute of Engineering & Technology, Ghaziabad, U.P*

[3] *School of Engineering and Technology, Sharda University, Greater Noida, India*

Abstract: In ancient times, humans were much predisposed to utilizing their hand-created tools to finish any kind of work. From the last few years, businesses related to production have been expanding. People began to rely on tools, machines, and smart gadgets to process their work, as these kinds of tools help them to achieve their target in the given time. . Since the 18th century, the world has experienced a lot of revolutions in industry across the globe. This type of growth in technology has made a base for industrial revolutions. New technology was introduced called "blockchain."Probably, blockchain technology is the most disruptive technology in the modern digital economy. The ability of blockchain technology has been greatly described in many research works, media, and majorly in the fields of finance and payment. One existing research is at the organizational stage, where it implements the architecture for internet safety as well as inconvertibility. "Industry 4.0" and "IIoT (Industrial Internet of Things)" are involved in its rising applications. Thus, in this paper, current applications of blockchain in IIoT as well as Industry 4.0 setups, existing open issues, modern application sectors, challenges related to IIoT, and their solutions are illustrated. The main focus of this paper is to empower and facilitate research in this field, which will help the developers in blockchain acquisition as well as investment in the "Industry 4.0" and "Industrial Internet of Things" space.

Keywords: Agriculture industry, Blockchain, Education industry, Food supply chain, Healthcare industry, Industrial revolution, Industry 4.0, IoT (Internet of Things), Privacy, Security, Scalability.

[*] **Corresponding author Nikhil Sharma:** HMR Institute of Technology & Management, Delhi, India; E-mail: nikhilsharma1694@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

1. INTRODUCTION

Undoubtedly, blockchain technology is an unpretentious invention. Blockchain structured the backbone of a modern kind of internet by permitting digital information to be disseminated but not replicated. Genuinely, invented for the digital currency, *i.e.*, Bitcoin, the tech organization has now discovered other efficient usages of this technology [1]. Thus, in simple words, a blockchain is a time-stamped sequence of inconvertible collections of information that is handled by a network of computers and not owned by any individual entity [2]. Each of these digital blocks is defended and limited to each other by employing a public database (*i.e.*, chain) [3]. In the network, by using cryptographic principles to keep data sharing safe, blockchain technology gives a decentralized database or digital ledger of transactions to everyone [4]. Basically, this network is a series of computer systems that must allow sharing before it can be authenticated and stored. There are many core elements of blockchain, but only the three most necessary elements are described. The first element is a block in which every chain includes several blocks, and each block has three fundamental components such as the data stored in the block is the first component [5]. A whole number of 32-bit is known as a nonce. In the second component, when a block is generated, it is randomly created which further ~~then,~~ produces a block header hash [6]. In third, a number of 256-bit called hash is wedded to the nonce. It must begin with a large number of 0s that is, it will be enormously small [7]. A nonce creates the cryptographic hash after the generation of the first block of a chain. The data in the block is considered as signed and forever linked to the nonce as well as hash until it is mined [8]. The second element is a miner. Through a procedure known as mining, miners produce fresh blocks on the chain. In a blockchain, every block has its own unrepeatable hash as well as a nonce, but also, it references the hash of the preceding block in the chain [9]. So, It is not simple to mine a block, specifically on huge chains. To solve the complicated math problem of finding a nonce that produces an admissible hash, special software is used by miners, because the nonce is only 32 bits and the hash is 256 bits. There are approximately 4 billion plausible combinations of nonce-hash that must be mined just before searching the correction [10]. When that occurs, miners have to search the “golden nonce” and their data is included in the database. Any kind of modification is accepted by all the nodes of the network and the miner is rewarded financially after triumphing mining of a block [11]. The third element is Node. Decentralization is one of the most significant topics in blockchain technology. The chain cannot be owned by a computer system or a company [12]. Rather, it is a disseminated ledger through which nodes are linked to the chain. Nodes (in any form of electronic gadget) manage replicas of the blockchain as well as maintains the functioning of the network. A major application of blockchain technology is to record financial information with a protected sharing.

There have been efforts to enucleate as well as expand the usages of the blockchain technology beyond the field of finance and to other sectors namely, supply chain, automobile, healthcare, production, education, and banking [13]. It is widely classified that, “Blockchain 1.0” is typically linked with digital currency, for example, smart contracts, Bitcoin.“Blockchain 2.0” is connected with the help of automated digital finance processes, and also, the popular technology *i.e.* “Blockchain 3.0”. It is concentrated on considering the requirements of the digital community like smart homes, smart banking, smart cities, and Industry 4.0 [14]. The fourth industrial revolution is hugely powered by IoT and other associated technologies. Here is another concept of IIoT (Industrial Internet of Things) or Industrial IoT which has a more particular concentration while the fourth revolution of the industry is basically linked with an intelligent industry arrangement. The conversion from conventional industry to intelligent industry or IndustrialIoT is supported by the inter-associativity as well as the digitalization of our community and spreading of IoT gadgets [15].

The other sections of the chapter are organized as follows, Section 2 illustrated “Industry 4.0”, its evolution from Industry 1.0 to 4.0, “Industrial Internet of Things (IIoT)” and major differences between the fourth revolution of industry and IIoT. Then, in section 3, some major applications of blockchain with some primary issues are described in different sectors such as healthcare and agriculture along with some of the existing open challenges in adopting blockchain in the IIoT technology. Modern application sectors in Industrial IoT or Industry 4.0, where blockchain technology is being executed for finding plausible solutions, are described in section 4. Furthermore, sections 5 and 6 present some of the major challenges related to the implementation of IIoT, and solutions to deal with the implementation issues in detail. And finally, a conclusion is discussed in section 7.

2. BACKGROUND MATERIALS

This section discusses the Evolution of Industry 4.0, and the comparison between IIoT and IoT.

2.1. Industry 4.0

In every day of humans’ life, technology plays a significant role. It has made it plausible for data access to be much faster. The atmosphere of businesses is getting involved in this frequent evolution of technology. Gradually, the industrial field has been consolidating greater applications of automation and associativity. For 2020, “Industry 4.0” was proposed in the year 2011, at the Hanover event,

CHAPTER 7

Enhancement of Iot Security Solutions Using Blockchain Technology

K. Sheela[1,*] and **C. Priya**[2]

[1] *Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India*

[2] *Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India*

Abstract: A blockchain is a growing list of records, called blocks, which are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. It is a decentralized, distributed and public digital ledger that is used to record transactions across many computers called nodes. Blockchain, in collaboration with the technologies like Artificial Intelligence, the Internet of Things, Big data, *etc.*, provides more effective outcomes by minimizing manpower with an increase in its feasibility. IoT is all about expanding the power of the internet beyond computers and smartphones to a whole range of other things, processes, and environments. Our day-to-day life can be made interesting with the applications of IoT-enabled devices in the home, agriculture, logistics, industries, healthcare sectors, and so on. They can be combined with the disciplines like data collection, management of huge data, storage of data, data analytics, *etc.* These IoT devices are embedded with sensors that are vulnerable to hackers and malware. At present, we cannot give complete assurance of the security of the access and data associated with the devices as it is possible for an intruder to misuse or mishandle the scheduled process. But, in association with blockchain technology, we can acquire solutions for problems related to security.

Keywords: Application, Authenticity, Blockchain, Banking sector, Consensus, Corda, Crypto-currency, Cryptography, Distributed, Ether, Ethereum, E-governance, Hashing, Healthcare, IoT, Platforms, Proof of work and stack, Security, Smart contract, Smart city.

1. INTRODUCTION

IoT devices have become a regular component in our day-to-day life. We can see that the devices which are connected` to the internet are gradually increasing by

[*] **Corresponding author K. Sheela:** Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India; E-mail: ksheela.research@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

paving the way for a digital environment. The traditional database provides a centralized architecture, whereas blockchain provides a distributed peer-to-peer network. In simple terms, blockchain is a collection of data stored in a database that maintains the continuously growing records in a distributed, peer-to-peer network node [1]. This makes the Blockchain and IoT to get integrated to provide even better services. Generally, IoT devices are liable to many kinds of security attacks [2]. The following are some of the attacks which occur to the devices connected to the internet.

Brute Force Attack: It is the process of trying all the possibilities of the password given by the authorized user.

The Man in the Middle: In this kind of cyber-attack, an intruder involves himself in the communication and gain access to the messages transferred. It is also possible for him to alter the messages which lead to miscommunication.

Denial of Service: This attack is used to slow down the process which also affects the reputation of an organization. Distributed Denial of Service (DDoS) may also occur to engage the resources in unnecessary services and makes the network resources unavailable for the appropriate activities. One of the methods to overcome this is proof of Activity which is the combination of PoS and PoW [3].

Eavesdropping: It is also known as sniffing or snooping attacks. It is the process of stealing the information while it gets transmitted over the network by devices like a smartphone, computers, or other connected devices.

Sybil Attack: It is the process of creating large numbers of pseudonymous identities to hide real identities and slow down the process. It entirely damages the operation of the network.

These attacks can be overridden by collaborating blockchain technology with the Internet of Things having the features like decentralized framework, immutability, reliability, autonomous behavior, and so on [4]. Every transaction in the blockchain is cryptographically sealed using public/private keys. Every transaction must be defined and authenticated. With these transactions, blocks must be created, validated, and linked (chained) [5] to enhance the security level of the transactions.

Blockchain technology, in collaboration with technologies like Artificial Intelligence, Internet of Things [IOT], Bigdata, *etc.* provides more effective end results by minimizing the manpower with an increase in its feasibility. Certainly, Blockchain entitles IoT devices by providing security and authentication with transparency in IoT ecosystems. We can easily predict that IoT will become a part of our day-to-day life in our near future with its huge development and collaboration with effective technologies like blockchain technology. Fraudulent activities may also occur in the localization of IoT devices where the location of the connected device might be tampered with to provide erroneous data. It can be overridden by this blockchain technology [2]. It is well-known specifically for its unique features like decentralized and distributed nature, hashing and cryptographic techniques, and smart contracts maintained between them. Let us have a deep look into this collaboration in this chapter.

1.1. Contribution of the Work

This chapter elaborates on security enhancement solutions and sheds light on the platforms where blockchain technology can be implemented.

Furthermore, it consolidates the features of these technologies and

highlights the study on collaborating Artificial Intelligence, Blockchain, and the Internet of Things for a sustainable environment.

It also encapsulates research directions along with certain guidelines.

1.2. Paper Organization

In section 2, we have discussed the platforms which can be used for implementing blockchain technology along with IoT integration. Further, in section 3, a number of techniques for imposing security for an operation have been explained with diagrams and tabular columns. A detailed explanation of IoT implemented with blockchain technology in various fields like smart city, healthcare, e-governance, education system, waste management, supply-chain management, *etc.*, has been elaborated in section 4.

2. PLATFORMS TO IMPLEMENT BLOCKCHAIN TECHNOLOGY AND ITS USES

By considering the nature of the Blockchain, it has been classified into three types, namely private, public, and consortium. A private blockchain is a restricted one. The user, who can access the data, will be assigned by a network administrator and others will be restricted from accessing it. There is no restriction of access in the public blockchain. The consortium is a semi-restricted blockchain where access permission will be given with certain restrictions to work

CHAPTER 8

Secured IoT Model for Sensitive Data Transmission Using Blockchain Technique

Vejendla Lakshman Narayana[1,*], **R.S.M. Lakshmi Patibandla**[2] and **Arepalli Peda Gopi**[1]

[1] *Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India*

[2] *Department of IT, Vignan's Foundation for Science, Technology and Research, Andhra Pradesh, India*

Abstract: Global progress in terms of technology involves dumb physical objects that communicate and solve intelligent species problems for us. The thrilling world of the 'network of things' or the Internet of Things (IoT) is certainly a safe place to feel and fulfill our needs. Communication technologies for machine-to-machine(M2M) enable autonomous networking between devices without human intervention. Such autonomous control is of vital importance for a range of Internet of Things (IoT) implementations, including smart manufacturing applications, healthcare systems, and home automation, to name a few. The Internet of Things has attracted almost everyone's attention because of its ability to track and influence the environment. One of the key features of any IoT system is its ability to connect and exchange data with other devices. In particular, IoT devices are using wireless networking to communicate with other devices. In this test, it tells us how IoT technology can communicate with our lives. The proposed method uses Secured IoT Model for Efficient Data Transmission using Blockchain Technique(SIoTM- EDTB) to provide security to the data during transmission. The proposed model is compared with the traditional method, and the results depict that the proposed model exhibits better performance.

Keywords: Attacks, Blockchain, Data loss, Data transmission, Security model.

1. INTRODUCTION

The IoT is a new computing paradigm aimed at turning ordinary daily objects into intelligent objects. IoT was described as one of today's transformative innovations that will change our vision, interpretation, and reaction to the changes in the environment around us. Advancements in omnipresent and widespread compu-

[*] **Corresponding author Vejendla Lakshman Narayana:** Vignan's Nirula Institute of Technology & Science for Women, Peda Palakaluru, Guntur-522009, Andhra Pradesh, India; E-mail: lakshmanv58@vignannirula.org

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

ting, integrated devices, communication, Sensor networks, and Internet-based protocols underlie the development and enablement of IoT in ordinary devices [1]. As a result, these technologies are usually known as technology enabling IoTs [2]. The authors examine, with a special focus on their characteristics, capabilities, strengths, and issues of different wireless communication technologies widely used in IoT devices.

The IoT paradigm is not a new technology but rather a combined 20 nations of approaches that benefit from research developments in semi-controllers, networking, and the processing of information [3]. If you are able to take a data center, you can use IoT to produce context-centric data and transmit it to another device or cloud where it is processed and mined to extract secret knowledge [4]. If you are able to accept the data center, you can use IoT to create new devices as well as new physical objects. This will then enable new technologies and applications to be created. In facilitating the wireless sharing between the IoT devices and the portal, and then the gateway to the remote repository via Internet, Machine-to-Machine (M2M) communication technologies play a vital role. In view of the limited battery capacity of IoT equipment, it is clear that the energy efficiency of wireless communication is very important: both duty cycle and energy-recovery solutions are extensively examined.

The Internet of Things is focused on conventional telephone networks and other knowledge providers. IoT is an extension of the Internet. The Internet terminal is a computer (PC, server) running all sorts of programs [5]. The Internet is nothing more than the encoding and transmission of data between the machine and the network [6]. There is no other terminal (hardware) on the Internet. The Internet is still the main concept for IoT. Unlike the Internet, there are not only PCs and servers, but even built-in computer systems and their help sensors can be viewed as terminals [7]. It can link all sorts of independent objects and make them work together in order to achieve a functional interconnection network.

Blocks are the technology's main principles. In the scheme, there are small collections of transactions. Each new block contains a reference to the previous transaction, including the previous transaction's SHA-256 hash [8]. This creates a 'chain' of connections . Blocks are difficult to build computationally and need several specialized processors and a considerable amount of time to produce. Due to the difficulty in creating a block and to the interference from one block, you need to manipulate the previous block and follow the chain to alter it altogether.

The proposed model introduces Secured IoT Model for Efficient Data Transmission using Blockchain Technique. In the proposed model, data transmission is secured as the blockchain technology is used for locking the completed transmission so that nodes' behavior is also monitored [9 - 12]. The introduction section gives a brief introduction of IoT and Blockchain and the remaining chapter is organized as a literature survey and then the proposed model that explains the process of secure data transmission framework, and then results are discussed and finally the conclusion of the chapter is given.

2. LITERATURE SURVEY

The new wireless communications system for green intelligent cities has been proposed by Bedogni *et al*. [6]. As IoT devices are used to plan, manufacture information, and monitor the energy supply and demand of households, IoT plays a key part in their plan. Although it was not mainly aimed at analyzing the communication systems used in IoT, they were assessed because they played a major role in the final implementation. The evaluation conducted in that work is quite superficial and focuses not on contact but the transfer of wireless power [13 - 15]. Moreover, not all available technologies are taken into consideration for assessment since they primarily focus on the SDN (SDN) architecture for heterogeneous IoT applications.

The study examined systems like cellular networks, short-range multi-shop technologies, and low-power (LPWA) technologies in order to use them for intelligent city implementation. The key weakness of these communication technologies is the failure to implement large-scale in restricted fields [16]. It was also suggested that these limitations can be resolved with various network optimization methods, including cell zooming, HetNets implementation, and context-aware content delivery [17 - 19].

The survey is similar to our study, although it has quite a different subject since it is based primarily on cellular technology and examines in detail the state-of-art criteria for 5 G; our work offers, compared to this, a more general classification of the M2M scenario (*e.g.* in the light of shorter distance 110 and capillary technology). Data sensor management and information extraction are very important in the second group [20 - 22].

The industry has been carefully studying and classifying industrial context-conscious technologies and applications ranging from localized products to manufacturing and healthcare [23 - 25]. Crowdsensing techniques are explored on the convergence of IoT, context-aware computing, and mobile devices.

3. PROPOSED MODEL

Blockchain – a decentralized dispensed headline – is a breakthrough technology capable of addressing IoT security challenges. A blockchain-based IoT network

CHAPTER 9

Transforming OTT Digital Platform Business Using Blockchain Technology

J.S. Shyam Mohan[1,*], **Nagendra Panini Challa**[2], **Pasumarthy Swathi**[1] and **Nuggu Kowshiki**[1]

[1] *Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India*

[2] *Department of Information Technology, Sri Vishnu Engineering College for Women, Bhimavaram, Andhra Pradesh 534202, India*

Abstract: Technology is becoming an indispensable part of our lives. It plays an important role in health, banking, and education. Organizations have started adopting these technological developments to satisfy customer needs. The rise of the Over-th--Top (OTT) digital platforms has created an economic platform in which the digital content, services, and offerings are facilitated by intermediaries and has changed the way of interaction. The blockchain serves as a means for creating a digital platform by creating trust among the intermediaries. Organizations should carry out innovative technology practices to be successful in a competitive environment. This chapter examines the gap between blockchain platforms and the role of the digital transformation process. It thereby provides researchers a holistic approach for studying the impact of blockchain on OTT platforms.

Keywords: Blockchain technology, Digital technology, Over-the-Top.

1. INTRODUCTION

Over-the-Top (OTT) is a term used in the media industry when TV is used to reach individuals' homes through physical links and boxes, and advanced content was conveyed through the web 'over the top' of the links and boxes. OTT has two products, the content and the viewers or the subscribers. Data collected from various locations is processed using Big Data analytics for enhancing and improving the customer viewing experience. Compared with steady competition from traditional television, the future of OTT platforms across the world looks bright.Traditional TV has started innovating by adapting to newer technologies to reach out to a wider range of audiences. Over the last decade, traditional TV has

[*] **Corresponding author J.S. Shyam Mohan:** Department of Computer Science and Engineering, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya (SCSVMV), Tamil Nadu 631561, India; Tel: ???????; E-mail: jsshyammohan@kanchiuniv.ac.in

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

started including OTT platforms as a part of their service offered to the consumers. AIB Research states that the video market across the world will keep on increasing at a fast pace with over-the – Top (OTT). By 2022, the OTT market will produce massive revenue of $51.4 billion with a surge CGAR (Compound Annual Growth Rate) of 10%. Subscribers will enjoy most of the benefits of OTT provided if they subscribe to the OTT platforms. In countries like North America and Europe, TV channel broadcasters are providing OTT services to their customers to withhold them consistently. Virtual Multichannel Video Programming (vMVPD) is provided at relatively cheaper prices to all the subscribers [1]. Globally, the number of subscribers opting for OTT is increasing when there has been a decline in traditional TV. The Average Revenue per User (ARPU) for pay channels is expected to go down four times, probably by 2022. Thus, there is no doubt that OTT players are marching towards increasing their revenue by adding more number of subscribers. Amazon, Apple, DAZN, Facebook, Google, and Netflix have started investing in setting up their own production houses. There is a great demand for content in OTT platforms owned by broadcasters, going ahead to have deals between broadcasters and OTT providers [2]. Table (**1**) shows the industry report of FICCI- E&Y for the period 2020 [3].

Table 1. The FICCI-E&Y M & E Industry report 2020.

Customer Segment	**No. of Users (in Millions) in a Particular Year**		
	2018	**2019**	**2022**
Digital Content (users consume content only on digital platforms, do not access television)	2.5	8	14
Tactical Digital (Consume Pay-TV and at least one paid OTT service)	12	34	91
Bundled Digital (Consume Pay-TV bundled with telecom)	218	262	363
Mass consumers (Consume Pay TV & occasionally some free OTT content)	426	316	176
Free consumers (Do not pay for content)	180	190	220

The worldwide income for the OTT market is expected to increase from $62.0 million (in 2018) to $149.7 (in 2024), making it with an increase of 15.8% in compound annual growth rate (CAGR) [4]. Indian users are more inclined to freely available content than subscription platforms. Keeping this in mind, OTT players have come up with a pay-per-user model called subscription-based video on demand (SVOD) business models on a monthly or yearly basis. Simultaneously, many OTT players are trying to promote advertising – based on the video on demand (AVOD), while other OTT players are adhering to free business models and planning them to convert into paid users. A blockchain describes an ever-growing set of shared, maintained, digital records and verified by several participants. There is a myriad of blockchain species, but this one definition is suitable for most scenarios [5, 6]. Each set of digital records in a blockchain is grouped into dependent blocks in order. This means that attempting to modify a transaction in any block would usually require modifying all of the following blocks, a computation-intensive task that is economically feasible by design, taking into account a new block is added within minutes. This process makes the data more sure and as time goes by, more blocks are added. Since this unique record set is maintained continuously in several places or distributed, it is highly fault tolerant; there is no central party that attacks, shuts down, coerced, or (in many cases) sues [7]. This decentralization is absolutely essential to do this work; a blockchain 100% owned by a single entity provides barely incremental benefit. Blockchain technology owes its origin to the Bitcoin cryptocurrency. Ensuring consent around a permanent digital ledger without the participation of a trusted central authority was needed (such as a bank, e-payment provider, or government) in order to create "digital currency" [8, 9]. Without an authoritative party to keep the register, you had to design something really innovative so that someone couldn't copy and paste the way they spend their digital money twice. This feature of blockchain technology, or the ability to have a unique and truly owned digital resource, is a vitally important characteristic for brands and marketers. The "digital scarcity" of the blockchain technology not only supports the value of Bitcoin, but it also provides brands with a real bridge between the finite physical world and a numerically infinite world. Many companies see blockchain as an open platform [10]. Open blockchains, like those that support Bitcoin cryptocurrency and Ethereum network, rely on a new model to make up for the lack of a trusted broker. On the other hand, with their exploration of closed or "authorized" blockchains, financial institutions are fall to the top to adopt a technology that an anonymous individual or group invented to help render these institutions useless after the 2008 crash. Even in this digitally sterile implementation, banks can enjoy advantages such as quick settlement times and more quickly agreed trade finance terms by inheriting at least some of the characteristics of an open blockchain, such as immutability and decentralization.

In recent years, British Columbia has gained prominence in the industry and gradually to be recognized as a game-changer for many industries such as the service, financial, and manufacturing sectors [11]. Due to its specific features such as privacy, security, smart contracts, scalability, and the ability to resolve file double-spending problems, the need to make SCM more efficient becomes essential. The BC implementation improves the transaction between two or multiple parties in terms of confidentiality, monitoring, transparency, and

CHAPTER 10

Blockchain-based Cultivating Ideas for Growth: A New Agronomics Perspective

Vishakha[1], **Nikhil Sharma**[2,*], **Bharat Bhushan**[2] and **Ila Kaushik**[3]

[1] *HMR Institute of Technology & Management, Delhi, India*

[2] *School of Engineering and Technology, Sharda University, Greater Noida, India*

[3] *Krishna Institute of Engineering & Technology, Ghaziabad, U.P., India*

Abstract: The development of nourishment and food is an essential requirement of nations for their affluence and welfare. Agriculture is the science and specialty of developing plants and livestock. In sedentary human civilization, agriculture plays a key role. The agribusiness needs to do a ton of work to keep up and fabricate the purchaser's trust with regards to the food quality check. A blockchain-based agricultural arrangement holds a guarantee for the agro-business with its capacity to acquire clarity and transparency in the framework. Minimal effort agrarian protection plans are progressively seen as instruments for giving social assurance to the individuals influenced by floods or dry seasons. In assisting with the diminishing effects, they endure because of such occasions. Therefore, this chapter introduces the idea of blockchain technology, extensive literature survey, including a review of blockchain development in the nourishment sector followed by the cases in the food supply chain. This chapter presented various opportunities and an ideal architecture of how blockchain will function in the farming sector. Finally, the chapter concludes by featuring open research difficulties in this field.

Keywords: Agribusiness, Agriculture, Blockchain, Farming Insurances, Food Safety, Internet business of Agri Products, IoT, Nourishment Supply network, Smart Agriculture, Smart Contracts, Supply Chain, Traceability, Transaction Costs, Underwater fishing industry.

[*] **Corresponding author Nikhil Sharma:** HMR Institute of Technology & Management, Delhi, India; E-mail: nikhilsharma1694@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

1. INTRODUCTION

Apart from cryptocurrencies, blockchain exhibit a wide variety of applications. The innovations in the field of blockchain are surely transforming numerous industries from banking to the healthcare sector and also the real estate business. Now research works are going on to implement the same in the agricultural sector. With the advancement in IoT applications, the technological domain, as well as financial sectors have acquired substantial growth in ecological observing applications to assess the quality of water, soil, and air. The world population is calculated to be 7.8 billion as of April 2020. With the continuous increase in population, there is a drastic increase in the demand for per-capita food.

Studies in 2014-15 showed that an adult has a 6.1 percent more calorie urge as compared to that of an adult in 1975-76. Increasing demand for food has remarkably affected the environment, which as a result has endangered many species. The destruction caused to the environment due to high food demand is in the form of deforestation, increased levels of carbon emission, *etc*. If the food supply chain is efficiently organized then there is a potential of reducing carbon footprint and environmental hazards which in turn will guarantee food safety [1]. In the current food supply chain, there are several stakeholders involved from production to consumption, making the situation difficult to retrieve actual step-by-step data for analysis. It is presented in the reports that in agricultural farming activities, a significant amount of carbon is produced in various processes. In the United States, it is estimated that among all the factors responsible for the generation of greenhouse gases, only transportation of food contributes 11% to the emission. It is observed that food production must be doubled by 2050 to meet the nutrients requirement of every individual [2].

Due to the increase in the cases of food consumption diseases, now the consumers want to know detailed information about their eatables and others. People show very little reliance on the existing food system. Blockchain has provided exciting solutions for these problems. It provides eternal evidence for each proceeding part which is then arranged into various blocks and no changes can be reflected there. It also helps in replacing those physical trackers and monitoring entities to prevent the imprecise impact of the traditional supply chain [3]. Tracking of the supply chain is the most important measure to protect the safety of eatables, securing them from malign vulnerabilities and encouraging food certification. LetsFarm is a start-up utilizing computerized reasoning with AI to enable ranchers over the globe. It utilizes transparent instruments and advancements to associate farmers so they can get the data they need from any place. Appropriate data can assist farmers with increasing their yield and to have a better salary from similar harvests that they are developing. LetsFarm likewise engages farmers with auxiliary salary by giving crucial data and expanding the pay of farmer's family units. After all, the overall growth of ranchers is the progress of the country all in all!. The Dutch Ministry of Agriculture, Nature, and Food Quality financed the main research venture, "Blockchain for Agri-food" which has been proposed to investigate blockchain suggestions for Agri-food. Pilot research shows that blockchain innovation empowered nourishment to be followed from farm to market in only a couple of seconds [4]. Blockchain additionally assists with watching bottomless items and diminish instances of illicit gathering and delivery cheats. The United Nations uncovers that nourishment fakes cost the worldwide economy around $40 billion every year because of unlawful exchanges. A ton of advancements originated from new businesses and the rural division isn't a special case. Ripe.io and Pavo Coin are two ongoing business models that use blockchain in the supply chain [5].

Ripe.io is a new business situated in SanFrancisco. Ripo.io centers around farming and offers clients an elevated level of straightforwardness. The framework created by Ripo.io can distinguish mugginess, readiness, and the temperature of the item. In this way, the rancher gets the data about the states of things. Blockchain achieving decentralization is not entirely technical in nature rather it's a combination of technical and smart engineering incentives. It began in 2008 with Satoshi Nakamoto, whose real identity is still not known to anyone, released a white paper that introduced a purely peer-to-peer version of crypto cash called bitcoin. There are four types of blockchain named as a private blockchain, public blockchain, federated blockchain, and the last one being hybrid. In private blockchain access is controlled, only a few users have the permission to view and verify the transaction. It is used in services where data security is a prime concern [6]. A public blockchain is one that has open access to all though transactions are anonymous. Transactions are transparent to those who have view access in the ledger. Federated blockchain is operated by a group or federation and only the members of the group have access. Hybrid refers to the system which uses public blockchain but also hosts private blockchain. Though data is stored on a public blockchain yet data privacy is not intruded. There is an incentive that is provided to the nodes for behaving honestly. There are two incentive mechanisms in the bitcoin named block reward and the other is transaction payment. In the service of creating a block in the blockchain, initially, the creator of the block includes the generation of special coin transactions in the block and then chooses the receiver address of this agreement. Block maker gets to the opportunity to gather the reward only if the block terminates up on long-term consensus branch. In the blockchain, the worth of block reward gets halved after every four years. Block reward is how new bitcoins are made and it is assessed that it will run out in 2140. There will be no new bitcoins if this standard remains unchanged. In transaction

CHAPTER 11

Blockchain Solutions for Big Data Management

Deepak Kumar Sharma[1,*], **Saakshi Bhargava**[2], **Aashna Jha**[3] and **Sudhir K. Sharma**[4]

[1] *Department of Information Technology, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India*

[2] *Department of Physical Sciences and Engineering, Banasthali Vidyapith, Tonk, Rajasthan, India*

[3] *Department of Electronics and Communication, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India*

[4] *Department of Computer Science, Institute of Information Technology & Management, New Delhi, India*

Abstract: The managing of unprecedented growth of data in the growing world is an important task. Knowing that the world is facing development in the numerical aspects and multiplicity of digital data that are normally produced by both consumers and technologies, dealing with this huge amount of data and finding the finest way to store, process, and organize it is necessary. This is the point where blockchain comes into the picture by providing significant inputs as it is the decentralized system for private data. Certainly, several industry experts are considering blockchain and its welfare for many improvements in different fields. Big Data is the recklessly rising sector in the ecosphere as every industry wants to get an understanding of the customs arrangements of their customers, where Big Data mentions huge datasets that are examined to divulge fundamental outlines using progressive statistical representations and data mining. The data produced is of petabytes range and when we are dealing with such a large range of datasets, problems related to it arise and not only collection of data is focused but security measures are also given extra importance, and proper care of produced data is taken so that no malicious action takes place.

Keywords: Big Data, BIot, Bitcoins, Blockchain, Consensus Algorithm, Cryptocurrency, Cryptography, Data mining, Decentralization, Distributed ledger, Electronic Health Record, Immutable network, IoT, Peer to Peer Network, Private Blockchain, Proof of Stake, Proof of Work, Public Blockchain, Public Key, Smart Contracts.

[*] **Corresponding author Deepak Kumar Sharma:** Department of Information Technology, Netaji Subhas University of Technology, Dwarka, Delhi 110078, India; Tel: 9868861080; E-mail:dk.sharma1982@yahoo.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

1. INTRODUCTION

Blockchain and Big Data are two technologies that continue to expand at a phenomenal rate. Both have been developed separately and have largely been applied in various industries independently from each other. Blockchain applications have been centric towards cryptocurrency and bitcoins with their distributed ledger technology (DLT) attracting both tech enthusiasts and potential investors in this new area of business. It has further expanded into other fields such as banking and supply chain management, finding use in all spheres of life. Blockchain technology truly can disrupt the current economic system of the world by its decentralized structure and removal of the third party. Big Data has become a buzzword in recent years with data multiplying like never before. Its applications cannot be limited to just one field as data is utilized and generated everywhere. From sensors to social media websites, big data is everywhere around us. Challenges arise when it comes to utilization and analysis as it holds the key to vital information. This information invariably proves to be valuable to businesses and governments alike, studying the performance of their products and services.

The major contribution of the following chapter will be highlighting the:

- linking up of the two powerful technologies Blockchain and big data.
- focusing on how Blockchain technology can change the way we deal with big data and make it a much more efficient process.
- highlighting the variety of benefits such as ensuring data security and performing data analysis, - Blockchain's advent and its integration with big data can serve a variety of industries ranging from finance to medicine.

The paper is organized as follows. The introduction includes Mechanism, Contemporaneous advancements in blockchains, and the challenges it must face, it also includes the basics of big data, its types, and characterization which are focused on in the second part of the same section. Section 2 comprises how big data and blockchain can together make a difference. Section 3 highlights the applications when the two technologies are used together. The final two sections are completely dedicated to further advancements and the conclusion.

2. INTRODUCTION TO BLOCKCHAIN

Blockchain technology [1] has revolutionized the world in more than one way. It is safe to say that it has covered multiple and a variety of spheres ranging from the economy [2] to healthcare. The history of how blockchain came to be can be credited to Satoshi Nakamoto, who outlined the basic workings of the technology and since then it has continued being developed for a variety of applications. Ethereum took things a step further and developed the concept of smart contracts. Blockchain is often referred to as Distributed Ledger Technology (DLT). A simple way to look at it would be to take the example of a Google Doc or a Wikipedia Page. Here, our document is distributed amongst many and every person can make a change in real-time and any updates are visible and transparent to all. Since blockchain is based upon DLT and everyone has access to the ledger, the information is transparent thus increasing accountability [3].

A major advantage that blockchain [4] has over existing systems is that there are no transaction costs involved. Infrastructural costs to maintain the system exist but any user making any trade will not face any additional costs. This happens because blockchain cuts off any third parties owing to its decentralized system. This will have serious consequences in the future economic system considering that many businesses currently make a profit by being the third party connecting the consumer to the product. For example, a yearly subscription to any magazine will stop being popular as the user can just pay a very small amount per article considering no additional transaction costs will be levied.

Blockchain is quite literally what its name implies - a chain of 'blocks.' Here 'blocks' are digital pieces of information stored in a public database 'the chain.' Despite its growing significance in today's world, blockchain is not a new technology. It is in fact an amalgamation of three proven and existing technologies [5], explained in Fig. (**1**).

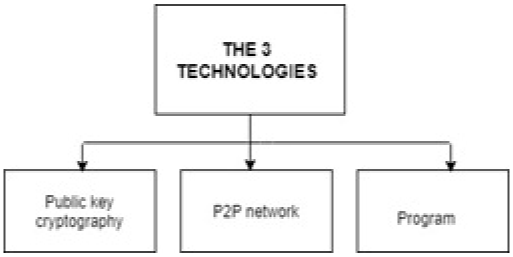


Fig. (1). 3 technologies.

The Peer to Peer Network is the defining feature of blockchain technology. The network is nothing, but a system of nodes connected and interconnected with each other. Each node is a computer network that can either take any input or perform functions and send its output. There is no hierarchy among different nodes and there is a uniform topology with the work being divided equally.

Public Key Cryptography [6] uses the concept of two keys, one public and one private. The public keys are as the name suggests public and distributed amongst

CHAPTER 12

Blockchain Security Solutions for IoT and Big Data

H. Abhijith[1,*], **Deepti Gupta**[1] and **Shilpi Sharma**[1]

[1] *Amity School of Engineering and Technology, Amity University, Noida, U.P., India*

Abstract: Technologies shaping the future, Internet of Things (IoT) and Big Data, are the leading research topics in the computer science department. Every field like this is prone to attacks from hackers and adversaries, which is why there is a need for proper security method implementations. The current nature of the Internet of Things uses centralized servers for data collection and analysis requirements, which invites many security concerns. Similarly, big data deals with a huge amount of data that is processed and analyzed every day. The blockchain network can fill this need for a better security solution. Even though it is in its infancy but due to the features, such as Decentralization, Persistency, Anonymity, and Auditability, it is able to strengthen the security of the various IoT and big data applications. This paper discusses the security flaws in the existing centralized infrastructure used by the above technologies and presents the security solution to solve the flaws.

Keywords: Big data, Blockchain, Internet of Things, Security solution.

1. INTRODUCTION

The Internet of Things (IoT) is a collection of interconnected computing devices, mechanical and digital computers, objects, animals, or unique identifiers (UIDs) that can transmit information over a network from one person or without the need for human-computer interaction. However, it comes with many security issues that have many similarities with the security of IT [1]. Many current IoT networks rely on centralized networking modes for connecting to servers or cloud services for data processing and storage. The fear is that the server will become a bottleneck and a new target for cyber-attack, as well as a failure point that will disrupt the whole network and harm the consistency of the tests. Consequently, it remains complicated how to create a fully reliable and interconnected ecosystem to support such embedded devices and computer resources for data transmission [1].

[*] **Corresponding author H. Abhijith:** Amity School of Engineering and Technology, Amity University, Noida, U.P., India; E-mail: abhijithrajihari@gmail.com

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

Big data is a concept describing the vast amount of data that inundates an enterprise on a regular basis- both organized and unstructured.

However, what is relevant is not the volume of information but what the organizations do with the said critical information. Some users use this info for their own gain and do selfish mining or share private information with companies. So, to overcome these issues with IoT and Big data, blockchain is implemented [2]. Blockchain is a decentralized system, which removes the use of a third party in a transaction thereby creating a peer-to-peer connection. It is based on functionalities like encryption, decentralization, immutability, and transparency. All the data stored in a blockchain is coupled in blocks like a database. All the transactions are connected with nodes. When a new transaction appears, the sender via a peer-to-peer network communicates it to all the different nodes. As the transactions are being validated, it is stored in the transactional pool. When the transactions are being validated in the pool, miners create a new block and store all the transactions thereafter which the block is mined [2].

This paper discusses the security flaws associated with IoT and Big data. It also tells about the possible security problems that are associated while implementing blockchain. This paper also gives some possible solutions to these problems. There are various examples to elaborate the idea of implementing and its various outcomes in this paper. We review some of the alternatives given by other papers like cloud-based drone systems for data collection [3] and Fair Access [4]. The paper focuses on the security solutions based on blockchain designed for an IoT network. These approaches include the security maintenance of IoT computers, safe firmware upgrades, and trust verification of a trustworthy computer base, authentication of IoT device identity, and secure data store access to control information systems. The paper also focuses on a Blockchain-based IoT Device Security Architecture in Smart Homes where the architecture consists of three levels, namely local smart home networks, an overlay network, and cloud storage [1]. Entities use blockchain transfers for coordination between themselves in each stage. This paper reflects on the IoT blockchain platform by analyzing future data interruptions and security issues during the interaction with IoT components. These security issues include confidentiality of data, lack of resources for design practices, inadequate information on upgrade and maintenance [5].

The paper is organized as follows:

Section II presents the literature related to the topic. Section III analyzes and discusses various security issues faced by IoT and big data, followed by a review of the proposed and implemented security solution of blockchain. Section IV discusses the growth of the security issues discussed in the previous section and how there is a need for a blockchain solution. Section V summarizes the related work. Section VI concludes the paper with an outline of open issues and future work.

2. LITERATURE REVIEW

In this section, we will discuss the various conclusion derived from the papers read as part of the background study.

A study conducted by [6], Zheng *et al.* raises various privacy issues and security threats like lack of optimally controlled role in communication between the devices in the IoT to prevent hijacking and cyberattacks, fairness in data collection and use, and identification in IoT. These challenges can be solved by blockchain as it enables a decentralized or a distributed network. However, it also brings out challenges like a proper ledger storage facility, severe inadequacy of appropriate legal standards, and limited research in the technology. Karafiloski *et al.* [7] discuss some major characteristics that build up a blockchain network such as auditability, anonymity, persistency, and decentralization. These characteristics help to build a secure network, which can be used for Big Data and IoT. A proper consensus algorithm is key to a successful blockchain network. An efficient consensus algorithm provides safety and convenience. There are also the same challenges that occur while using a blockchain network some of which are scalability and privacy leakage (Table **1**).

Table 1. Summary of Literature Review.

S. No.	Title	Conclusion	Gap Identified
1	Blockchain Solutions for Big Data Challenges	Blockchain gives the user control of all their data and transactions. This concept can influence Big Data to find a solution for storing and managing data in a distributed manner on a P2P network.	The paper mentions the use of healthcare without considering the heavy computational cost of using a blockchain network in time-critical events.
2	Making Big Data Open in Edges: A Resource-Efficient Blockchain-Based Approach	The key concept of Proof-o--Collaboration is that participants contribute to the big data sharing so that they can also benefit from other participants' collaboration.	The mentioned PoC mechanism model considers the blockchain as an entity, which is an extreme case.
3	A Survey on the Security of Blockchain Systems	Blockchain 2.0, where the use of smart contracts is enabled, have problems like Criminal smart contracts, Vulnerabilities in a smart contract, Under-optimized smart contract, Under-priced operations.	A major advantage of a smart pool is its ability to prevent pool hopping which could have been mentioned.

SUBJECT INDEX

Sudhir K. Sharma, Bharat Bhushan, Parma N. Astya and Narayan C. Debnath (Eds.)

SUDHIR K. SHARMA

Sudhir K. Sharma is currently a Professor in the Department of Computer Science, Institute of Information Technology & Management affiliated to GGSIPU, New Delhi, India. He has extensive experience for over 19 years in the field of Computer Science and Engineering. He obtained his Ph.D. degree in Information Technology from USICT, GGSIPU, New Delhi, India. Dr. Sharma obtained his M. Tech degree in Computer Science & Engineering in 1999 from the Guru Jambheshwar University, Hisar, India and M.Sc. degree in Physics from the University of Roorkee (now IIT Roorkee), Roorkee, in 1997. His research interests include Machine Learning, Data Mining, and Security.

BHARAT BHUSHAN

Bharat Bhushan is an Assistant Professor of Department of Computer Science and Engineering (CSE) at School of Engineering and Technology, Sharda University, Greater Noida, India. He received his Undergraduate Degree (B-Tech in Computer Science and Engineering) with Distinction in 2012, received his Postgraduate Degree (M-Tech in Information Security) with Distinction in 2015 and Doctorate Degree (PhD Computer Science and Engineering) in 2021 from Birla Institute of Technology, Mesra, India. He has published more than 80 research papers in various renowned International conferences and SCI indexed journals. He has served as Keynote Speaker (resource person) numerous reputed international conferences held in different countries including India, Morocco, China, Belgium and Bangladesh.

PARMA N. ASTYA

Parma N. Astya is a dean of the School of Engineering Technology at Sharda University Greater Noida. He has over 26 years of teaching, industry, and research experience. He has expertise in Wireless and Sensor Network, Cryptography, Algorithm, and Computer Graphics. He obtained his Ph.D. degree from IIT Roorkee and M.Tech & B. Tech in Computer Science & Engineering from IIT Delhi. He has been an ex-president of the National Engineers Organization. He also has active memberships of ACM, CSI, ACEEE, ISOC, IAENG, and IASCIT.

NARAYAN C. DEBNATH

Narayan C. Debnath is currently the Founding Dean of the School of Computing and Information Technology at Eastern International University, Vietnam. Dr. Debnath has been the Director of the International Society for Computers and their Applications (ISCA) since 2014. Formerly, Dr. Debnath served as a Full Professor of Computer Science at Winona State University, Minnesota, USA for 28 years (1989-2017). Dr. Debnath earned a Doctor of Science (D.Sc.) degree in Computer Science and also a Doctor of Philosophy (Ph.D.) degree in Physics. Dr. Debnath is an author or co-author of over 425 publications in numerous refereed journals and has been a visiting professor at universities in Argentina, China, India, Sudan, and Taiwan.