Pegem Journal of Education and Instruction, Vol. 13, No. 4 , 2023 (pp. 674-694)

RESEARCH ARTICLE WWW.PEGEGOG.NET

AN EFFECTIVE PRIVACY-PRESERVING BLOCKCHAIN ASSISTEDSECURITY PROTOCOL FOR CLOUD-BASED DIGITAL TWIN ENVIRONMENT

P.Revathi, [1], Yeleti Anitha,[2] Palapothu Sushmitha[3], Varakala Dixitha[4]

[1] Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad swecrevathi@gmail.com

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT: In the DT setting, you may run virtual simulations of physical objects by creating a copy of them. There has been an uptick in the use of DT in a variety of contexts— medical, healthcare, manufacturing, aerospace, etc.—thanks to its conceptual development, predictive maintenance, real-time monitoring, and simulation capabilities. The use of DT has many benefits, but it has also introduced significant security risks. This goal has motivated the development of a number of authentication methods tailored to DT settings, each with its own set of security and privacy considerations. Using blockchain technology, this essay first examines a newly suggested two-factor authentication technique for DT settings. Unfortunately, the examined method falls short in providing the desired level of security and is vulnerable to a number of security attacks, such as those that target anonymity properties, smart card theft, offline password guessing, and known session-specific temporary information attacks. The fact that an attacker may pose as the legitimate owner, user, and cloud server of the protocol under scrutiny is also shown. We provide a strong three-factor authentication solution that protects user privacy in DT settings to solve these security gaps. By running the RealorRandom (ROR) model, the informal security analysis, and the formal security analysis utilizing the well-known Burrows-Abadi-Needham (BAN) logic, we show that the suggested work is safe. The proposed framework outperforms the current schemes in terms of security features, computing costs, and communication costs after a thorough comparison with existing competing schemes, including the studied system. **KEYWORDS:** DT environment, Burrows-Abadi-Needham (BAN) logic, Real-orRandom (ROR) model, Predictive maintenance , Real-time monitoring.

1. INTRODUCTION

An accurate digital representation of a physical system that can be updated in realtime is called a digital twin. In the DT setting, you may run virtual simulations of physical objects by creating a copy of them. The concept of using a clone in a virtual environment for simulations was first put forth by Grieves and Vickers in 2002. In 2010, the National Aeronautics and Space

How to cite this article: P.Revathi, 1, Yeleti Anitha,2 Palapothu Sushmitha3, Varakala Dixitha4. AN EFFECTIVE PRIVACY-PRESERVING BLOCKCHAIN ASSISTEDSECURITY PROTOCOL FOR CLOUD-BASED DIGITAL TWIN ENVIRONMENT.Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 674-694

Source of support: Nil **Conflicts of Interest:** None.

DOI: 10.48047/pegegog.13.04.78

Received: 12.10.2023

Accepted: 22.11.2023 **Published:** 24.12.2023

Administration (NASA) used the term "DT" to describe this approach [2]. Industrial Internet of Things (IIoT) and Industry 4.0 are two paradigms that might benefit from the DT concept's development. The goal is to provide a unified interface for automated discovery and transmission of all data sources and control interface descriptions pertaining to products or processes. Analyzing the DTs of the integrated components allows developers and engineers to build, integrate, and establish the necessary interfaces, communication linkages, and integrations without having specialized knowledge of each component [3]. A human engineer may become unnecessary in the future when the gadgets can find and interact with each other on their own. Such autodiscovery and auto-established connection, facilitated by DTs, has the potential to make the Internet of Things (IoT) more scalable in the long run, opening up hitherto unthinkable uses. The industrial, construction, healthcare, and space sectors are among the many that are investigating DT technology. The Internet of Things (IoT) and mobile devices are now part of the DT technology's scope of use. For example, in a vehicle setting, it is possible to accomplish autonomous driving, and in a medical setting, it is possible to provide accurate and thorough remote medical treatment.An accurate digital representation of a physical system that can be updated in real-time is called a digital twin. In the DT setting, you may run virtual simulations of physical objects by creating a copy of them. In 2002, Grieves and Vickers first suggested the concept of running virtual simulations with a clone; in 2010, the National Aeronautics and Space Administration (NASA) used the term "DT" to describe the approach. Industrial Internet of Things (IIoT) and Industry 4.0 are two paradigms that might benefit from the DT concept's development. The goal is to provide a unified interface for the definition of control interfaces and all data sources pertaining to products or processes so that they may be automatically discovered and communicated with.

2. MATERIALS AND METHODS:

One of the most promising advancements in healthcare is the application of digital twin technology, offering valuable applications in monitoring, diagnosis, and development of

treatment strategies tailored to individual patients. Furthermore, digital twins could also be helpful in finding novel treatment targets and predicting the effects of drugs and other chemical substances in development. In this review article, we consider digital twins as virtual counterparts of real human patients. The primary aim of this narrative review is to give an in-depth look into the various data sources and methodologies that contribute to the construction of digital twins across several healthcare domains. Each data source, including blood glucose levels, heart MRI and CT scans, cardiac electrophysiology, written reports, and multi-omics

data, comes with different challenges regarding standardization, integration, and interpretation. We showcase how various datasets and methods are used to overcome these

obstacles and generate a digital twin. While digital twin technology has seen significant progress, there are still hurdles in the way to achieving a fully comprehensive patient digital twin. Developments in non-invasive and high-throughput data collection, as well as advancements in modeling and computational power will be crucial to improve digital twin systems. We discuss a few critical developments in light of the current state of digital twin technology. Despite challenges, digital twin research holds great promise for personalized patient care and has the potential to shape the future of healthcare innovation. Digital twin technologies have seen a rise in popularity in various industries, including manufacturing, engineering, and rocketry, from where the term originated [1]. This rise can be attributed to the developments in rapidly collecting, storing, and sharing data, together with computers being able to apply complex models and algorithms in a short amount of time [2]. In several fields of healthcare, such as precision medicine, clinical trials, and public health, the application of digital twins has become more and more apparent as they may serve as a tool to understand and simulate complex physiological processes. Moreover, digital twins may also reduce the need for animal experimentation, which takes an estimated 200 million animals per year [3], as it allows a direct translation of in vitro measurements into what could be expected in vivo either in digital animal models or humans [4]. General definitions of a digital twin have been given in the literature [5,6,7,8,9]. In this narrative review, we work with the general definition of healthcare digital twins [10] as virtual replicas of real human patients, through which clinicians can gain valuable insights, optimize treatment strategies, and deliver personalized care [5,11,12]. For specific healthcare domains, the operationalization of this definition depends very much on the underlying methodology and data used to construct the digital twin. Though the general aim is expected to align with the definition above, a _*cardiac*‘ digital twin (e.g., Section 2.2 below) differs considerably from a _*drug response*‘ digital twin in methodology, data types, and implementation. One of our

goals is to take a deeper look into the methodological aspects underlying digital twins across several healthcare domains where this technology is being applied. By gaining an understanding of the methods and data used, the potential value and important pitfalls of digital twins in future studies can be more easily identified. Healthcare digital twins require large amounts of data and often multiple data types. These include measurements that can be made using a smartphone or watch, like heart rate, temperature, and location [13], and data that can otherwise be gathered at home, such as blood pressure and blood oxygen saturation, but also medical imaging data recorded during CT or MRI scans, electrophysiology, and various types of -omics data, which can be collected through a wide range of techniques including sequencing, immunoprecipitation and mass-spectrometry [14]. After generating the digital twin, a variety of methods can be applied to make simulations and predictions. These range from fitting regression lines to the data to designing deep neural networks [15] and can be used for many different purposes. Apart from their clinical use, digital twin technologies may also be applied to identify novel drug targets, simulate the effectiveness and safety of new treatments, or predict patient traffic during a pandemic [5]. The aim of this narrative review is twofold. We aim to review the methodological development of digital twin systems across several healthcare domains. Second, we aim to identify the types of data required to construct the respective digital twins. Secondary to these aims, we further discuss how to overcome the challenges introduced by handling large amounts of data and standardization, integration, and interpretation of many different types of data. The research questions we desire to answer are: (1) which data types and sources are important for the development of healthcare digital twins? (2) What are the prevailing methods and techniques employed in healthcare digital twin systems, and how do they vary in their applications? (3) How can the challenges related to healthcare digital twin methods and data be transformed into opportunities? Addressing these aims and questions will be crucial to harnessing the full potential of digital twins, ensuring that this promising idea can be integrated successfully into clinical practice. Digital Twins (DTs) are widely discussed in the context of the Industry 4.0 paradigm as one of the main opportunities to strengthen the overall competitiveness of manufacturing enterprises. Despite a substantial scientific discussion, there is still no unified understanding regarding the constitution and subsequent usage of DTs within production logistics systems. Therefore, this paper focuses on the application of DTs in production logistics. The authors discuss common definitions, characteristics, and functionalities of DTs and outline current developments and implications from state-of-the-art implementation approaches, by using a systematic literature review. Moreover, based on the research findings,

the authors evaluate a set of DT case studies, identify current research gaps, and present potential directions for future research initiatives regarding the field of production logistics in manufacturing enterprises. In today‘s hyper-dynamic environment, the Industry 4.0 paradigm is reaching far beyond the basic concepts of automation by revolutionizing manufacturing enterprises especially in the areas of smart production and smart logistics. Moreover, Industry 4.0 is characterized by the vertical and horizontal integration of production and logistics systems as well as the merging between the physical and virtual worlds [1]. Industry 4.0 approaches can, therefore, be divided into digitalization, digital interconnectivity, and selfcontrolling systems [2]. Various technologies and technological concepts are discussed in production logistics, which can be classified as Cyber-Physical Systems (CPS), Internet of Things (IoT), interfaces, decentralized applications, real-time localization systems, automatic identification, virtual environments including Digital Twins (DTs), and applications of data science such as machine learning, data mining, and big data analytics [3]. Companies are challenged with increasing dynamics, structural complexity, increased uncertainties and risks, and multiple feedback cycles. This leads to difficulties in the optimal design and control of production logistics systems [4,5]. However, DT technology offers several approaches to overcome these problems [6,7]. Originally, the concept of a Digital Twin was presented at the University of Michigan by Grieves in 2003. It was first introduced as a concept for product lifecycle management (PLM). At this stage, it was not explicitly called a Digital Twin, but the paper described the idea and important components of such a system [8]. NASA has taken up this concept and described a Digital Twin in the technology roadmap for their flight system, to make comprehensive diagnostics and prognostics, enabling continuous safe operations over the life cycle of the system [9]. Furthermore, Glaessgen and Stargel described a Digital Twin for the next generations of NASA and U.S. Air Force vehicles, giving more detail [10]. Nevertheless, different fields of research adapt the original concept of a Digital Twin to their specific domain. Therefore, several publications discuss the application of DTs in production planning and control, maintenance, process design, layout design, product design, production process optimization, as well as prognostics and health management (PHM) [11,12,13]. This may also be the reason why there is no common definition of a DT [14]. One approach to finding a standardized and common definition of DTs has been elaborated by the International Organization for Standardization (ISO). According to this proposal, the basic idea of a Digital Twin is to create a digital representation of an observable system or element [15]. More specifically, other authors suppose it to mirror a product, process, or service in virtual space

[16]. Convergence between the physical and the virtual space is mandatory [17] to create a closed-loop interaction between these components [18]. A bidirectional communication enhances this convergence [17], as real-time data integration plays a key role for Digital Twins [19]. The concept of Cyber-Physical Systems (CPS) can be described similarly. Tao et al. compared the differences and correlations of the two concepts. DTs are often discussed in the engineering area and are more focused on virtual models (VMs) that enable one-to-one communication between physical and virtual parts. CPS on the other hand is more frequently discussed in the scientific area. To enable fusion and one-to-many communication between the spaces, CPS emphasizes 3C capabilities (computation, communication, and control) . The DT technology can also be seen as a key enabler for realizing a Cyber-Physical Production System (CPPS) Among many other application areas, there is great potential for use in production logistics processes . Nevertheless, the different views and possible applications of DTs in the various domains lead to the result that no common understanding is being formed for this technology and its potentials. This paper aims to achieve a clear delimitation of DTs for the area of production logistics, to analyze potentials based on a systematic literature review enabling discussion of the state of the art in this specific domain. In this regard, further developments in this area can be established based on the systematic evaluation of the current literature with a special emphasis on common implementation concepts. Furthermore, barriers and research gaps will be identified as a starting point for further research initiatives.The concept of digital twin (DT) has emerged to enable the benefits of future paradigms such as the industrial Internet of Things and Industry 4.0. The idea is to bring every data source and control interface description related to a product or process available through a single interface, for auto-discovery and automated communication establishment. However, designing the architecture of a DT to serve every future application is an ambitious task. Therefore, the prototyping systems for specific applications are required to design the DT incrementally. We developed a novel DT prototype to analyze the requirements of communication in a mission-critical application such as mobile networks supported remote surgery. Such operations require low latency and high levels of security and reliability and therefore are a perfect subject for analyzing DT communication and cybersecurity. The system comprised of a robotic arm and HTC vive virtual reality (VR) system connected over a 4G mobile network. More than 70 test users were employed to assess the system. To address the cybersecurity of the system, we incorporated a network manipulation module to test the effect of network outages and attacks;

we studied state of the art practices and their utilization within DTs. The capability of the system for actual remote surgery is limited by capabilities of the VR system and
insufficient feedback from the robot. However, simulations and research of remote surgeries could be conducted with the system. As a result, we propose ideas for communication establishment and necessary cybersecurity technologies that will help in developing the DT architecture. Furthermore, we concluded that developing the DT requires cross-disciplinary development in several different engineering fields. Each field makes use of its own tools and methods, which do not always fit together perfectly. This is a potentially major obstacle in the realization of Industry 4.0 and similar concepts. Industrial Internet and Internet of Things (IoT) have brought up a capability to measure and observe various phenomena. Data available from those has in turn created an opportunity to develop system modelling capabilities such as Digital Twins (DT). The concept of DT has emerged to make the physical things and related data sources accessible for software and users on digital platforms [2]. Terms used for similar or partially overlapping concepts include digital counterpart, virtual twin, virtual object, product agent, and avatar [3]. DT is argued to consist of three parts: physical product, digital product and the linkage between the physical and digital products

[4]. DT enables real time communication with the physical twin in both directions. Interested entities, such as processes or systems, can read data from the physical product via a DT, analyze the data and execute simulations. Vice versa, actuation commands, control signals and other data can be sent to the physical twin with the help of a DT. The DT contains a structured description of available communication and control interfaces of the physical asset. These interfaces can be accessed and harnessed for application specific needs by analyzing the DT and without accessing and examining the physical twin at the site. Apart from the communication aspect, a DT will serve as container of all existing data about the physical twin. The actual data, such as CAD model files, sales documentation and measurement data, technically exist in several different software and systems. The role of DT is to bring these various data stores accessible via a single interface. Furthermore, just like a physical object is always tied to specific location and time, a DT needs to incorporate location and time aspects despite of it‘s digital nature. These fundamental features are the core of a DT. The ultimate value proposition of a DT is to enable communication between devices and systems in real time and, more importantly, automatically. Without DT, setting up complex systems, such as our remote surgery system, would require specialists and experts for each product, device and software piece incorporated. By analyzing the DTs of the incorporated components, developers

and engineers can determine, design and create the required interfaces, integrations and communication links without specific expertise of each component.

Eventually, the devices might be able to discover and understand each other without any human engineer in between. This sort of auto-discovery and auto-established communication with the help of DTs could eventually make IoT more scalable for applications currently unimaginable. The underlying problems, beside the obvious technical one that such protocols and networking architecture are currently only under development [2], include authentication of each device and user, safety and security, data ownership issues, reliability, robustness and acceptable delays, among others. Solving these problems with DTs will enable the Industrial Internet and IoT to really add value to current systems and processes. We developed a novel prototype system to investigate what kind of communication link is required in a mission critical application. As a case application, we chose the specific task of remote surgery. Such operations require near zero latency and high levels of security and reliability [5] and therefore are a perfect subject for analysis in the context of DTs involved in achieving the required features and functionality. Defining proper DT architecture that has potential to succeed in every possible future application is an immensely ambitious task. This kind of analysis via specific prototype applications provides the necessary building blocks to eventually be able to determine the structure and architecture of DTs. Moreover, we could determine if mobile network supported medical operations are feasible. We collected experimental results about the functionality of the DT, different feedback technologies and usability of the system in test sessions with test users. Cybersecurity was studied with implementations regarding network security and user authentication and analyzing state of the art technologies and their consequences in development of DT concept. Based on the experiences gained during the development phase and experiments, we present ideas on how a DT should be designed to succeed in a mission critical application with special emphasis on the cybersecurity issues. In many cases, the subject of a medical operation is in critical state and delays might result in further traumas. Additionally, it might be expensive, inconvenient or impossible for the patient and the medical personnel to travel to a mutual location. In these cases, remote operations could prove useful and might be possible with modern technologies such as Virtual Reality (VR), robotics and communication via a DT over mobile networks. VR supported applications provide great feedback and a significant improvement compared to more traditional video link and instruction passing. The first commercial VR applications, such as Forte Technology‘s VFX1, were launched in 1994 [6]. Only recently have the required technologies advanced enough to bring the VR devices to really usable level [7]. The best devices are able to generate virtual worlds that appear and feel almost like reality [8]. Moreover,

monitoring various data points in real time from the user has become possible with smart phones and without extensive purpose-built sensor setups. This data can be used in
augmenting virtual realities with real life elements [9]. Current state of the art technology in robotic surgery includes Da Vinci system. It enables prostate cancer surgeries to be performed with a robot inside a patient. A VR controller device is situated close to the patient. A doctor has a VR view inside the patient and maneuvers a robot with special controller interface [10],

[11]. Furthermore, some surgeries have been performed remotely. One example is a cholecystectomy (surgical removal of gallbladder) performed over a distance of 6230 km between the surgeon and the patient in 2001 [12]. However, the connection used was specially set up for the particular operation, which means that using similar technology requires these connections set up beforehand in order to perform operations quickly on demand. The problems in remote control of robots in surgical applications include sufficient feedback for the surgeon, timely co-operation and communication with the remote and local teams, calibration of the control system with the patient and reliability, latencies and cybersecurity of the connection, among others. Using digital technology (in contrast to analog technology) enables digital concepts such as DT and AI in solving these problems and utilizing existing digital networks such as Internet and mobile networks. Remote surgeries using mobile networks has not been attempted to date. Such operations require exceptionally safe and trusted hardware, software and communication systems. With the onset of 5G mobile network technology, robotic telesurgery over 5G has become a research hotspot to resolve the various issues such as required human-machine interfaces, security, privacy and reliability [13]. In addition to contribution in development of DT concept, our prototype system brings remote surgeries over mobile networks closer to reality by providing solutions to the above mentioned problems.Achieving data integrity verification for large-scale IoT data in cloud storage safely and efficiently has become one of the hot topics with further applications of Internet of Things. Traditional data integrity verification methods generally use encryption techniques to protect data in the cloud, relying on trusted Third Party Auditors (TPAs). Blockchain based data integrity schemes can successfully avoid the trust problem of TPAs, however, they have to face the problems of large computational and communication overhead. To address the issues above, we propose a Blockchain and Bilinear mapping based Data Integrity Scheme (BB-DIS) for large-scale IoT data. In our BB-DIS, IoT data is sliced into shards and homomorphic verifiable tags (HVTs) are generated for sampling verification. Data integrity can be achieved according to the characteristics of bilinear mapping in the form of blockchain transactions. Performance

analysis of BB-DIS including feasibility, security, dynamicity and complexity is also discussed in detail. A prototype system of BB-

DIS is then presented to illustrate how to implement our verification scheme. Experimental results based on Hyperledger Fabric demonstrate that the proposed verification scheme significantly improves the efficiency of integrity verification for large-scale IoT data with no need of TPAs. With the wide popularity of Internet of Things (IoT) technologies such as smart cities, autonomous vehicles and smart grids, the number of devices connected to the Internet is rising overwhelmingly. According to Gartner‘s forecasts, there will be a 42% increase in IoT connections and $20 billion in spend from 2018 to 2020. How to collect [1], process, store and analyze these large-scale IoT data securely [2] has therefore become one of the most important issues for further applications of Internet of Things. Traditional distributed database systems cannot satisfy the requirements of data management in the IoT environment, and Cloud Storage Services (CSSs) arise consequently. With external storage of data, the integration of IoT and cloud eliminates the burden of local storage and supervision. However, cloud service providers can certainly gain control of users‘ data, which seriously threatens the security of data. As a result, integrity verification of IoT data is of great significance for effective cloud storage. Existing data integrity verification schemes for cloud storage are mainly based on hash functions [3], asymmetric cryptographic algorithms [4], and erasure codes [5]. Data integrity verification methods can also be divided into provable data possession (PDP) mechanism [4] and proofs of retrievability (POR) mechanism [6] according to whether it can correct wrong data after verification. These traditional methods often rely on trusted Third Party Auditors (TPAs) to execute auditing tasks and the burden of users during the verification phase can be decreased. For example, in Wise Information Technology of 120 (WIT120), massive electronic health records (EHR) are collected by wearable devices and then stored in the cloud. Before accessing health data, services providers usually offload the validation task to TPAs to guarantee data integrity. However, in real world scenarios, TPA is not completely trusted. Even with encryption methods [7] which can avoid the leakage of users‘ privacy, the quality and effectiveness is completely dependent on the credibility of TPA. Blockchain technology has recently emerged as one of the most promising technologies and attracted great attentions for its transparency, immutability, security and decentralization. Researchers have considered to execute integrity verification services in the decentralized blockchain network, where transactions can be performed with no need of a trusted TPA. Ethereum and Hyperledger Fabric are two popular frameworks for the implementation of

blockchain network [8]. However, there is a significant scalability barrier for blockchain related applications, which limits their capability to support services with large-scale and frequent transactions, e.g., the computational and communication overhead during integrity verification for large-scale IoT data [9]–[11]. Besides, dynamicity of IoT data [12], [13] has seldom been investigated for most of the existing blockchain based data integrity methods. In order to address the problems above, we propose a Blockchain and Bilinear mapping based Data Integrity Scheme (BB-DIS) for large-scale IoT data in cloud storage. Main contributions of this paper are listed as follows:

- A blockchain based data integrity verification framework is proposed for large-scale IoT data. An associated series of protocols followed with verification algorithms and performance analysis are also presented in detail.

- A prototype system is built with an edge computing processor in the vicinity of the IoT devices to preprocess the large-scale IoT data so that communication cost and computation burden can be reduced significantly.

- Multiple simulation experiments are conducted on Hyperledger Fabric. Comparative analysis on computational and communication overhead among BB-BIS and other baseline schemes is given. Various sampling strategies are introduced, and optimized sampling verification scheme is finally recommended.

Despite the rapid development of cloud computing for many years, data security and trusted computing are still the main challenges in current cloud computing applications. In order to solve this problem, many scholars have carried out a lot of research on this, and proposed many models including data integrity test and secure multi-party calculation. However, most of these solutions face problems such as excessive computational complexity or lack of scalability. This paper studies the use of blockchain techniques to improve this situation. Blockchain is a decentralized new distributed computing paradigm. Applying blockchain technology to cloud computing, using the security mechanism of the former to improve the performance of the latter's secure storage and secure computing is a promising research topic. In this paper, the distributed virtual machine agent model is deployed in the cloud by using mobile agent technology. The virtual machine agent enables multi-tenants to cooperate with each other to ensure data trust verification. The tasks of reliable data storage, monitoring and verification are completed by virtual machine agent mechanism. This is also a necessary condition for building

a blockchain integrity protection mechanism. The blockchain-based integrity protection framework is built by the virtual machine proxy model, and the unique hash hash value corresponding to the file generated by the Merkel hash tree is used to monitor the data change by means of the smart contract on the blockchain, and the data is owned in time. The user issues a warning message for data tampering; in addition, a "block- and-response" mode is used to construct a blockchain-based cloud data integrity verification scheme. In the new generation of information technology, blockchain technology will be the key to breaking the problem [1]. At present, blockchain technology is becoming a frontier field of high value with its unique technological advantages, innovative value concepts and wide application scenarios [2, 3]. Many experts even believe that blockchain technology is expected to become the technology that has the potential to trigger the next wave of disruptive revolutions after steam engine, power, information and Internet technology [4]. Blockchain can solve the problem of trust mechanism. Trust is a key element of blockchain technology. It is more like a public account book that everyone can record, view, and maintain. Any record has a permanent time stamp and cannot be tampered with [5]. It is precisely because the blockchain technology has broken the centralization characteristics of the traditional Internet that the crisis of trust that plagues the modern economy has been solved to some extent. When the transaction is executed and resolved on the ledger, the parties themselves do not need to establish a trust relationship, but only need to trust the blockchain itself to achieve this goal. Blockchain can solve the problem of data authenticity. Blockchain can effectively promote data circulation and sharing[6]. Blockchain can effectively promote data production convergence. The blockchain led us to open the door to the "value Internet." The emergence of the Internet has made the means of information dissemination leap, and information can flow efficiently on a global scale without third-party and peer-to-peer implementation. The efficiency of value transfer has not been improved simultaneously. The birth of the blockchain is the beginning of human beings building the Internet worth equal to the information Internet. The value of the Internet will lay the foundation for the entire human society to enter a transparent and reliable credit society. Since the emergence of the concept of big data, data science and technology has developed rapidly. At the same time, the big data field is also facing certain problems [7-9]. Especially in the collaborative sharing of data, data transactions and data privacy protection. In the face of these problems, there are currently some solutions, but these solutions are centralized, that is, through some trusted third-party organizations to deal with the problems faced in data processing. However, there are other problems. The so-called trusted third-party organization

is really credible. Once a trusted third-party organization is doing evil, it will cause huge losses to users and data owners involved in data processing. The tripartite organization has enormous rights. Once the third-party trusted organization is controlled by the hacker, it will undoubtedly cause some losses to the user. The combination of blockchain and big data will provide solutions to the problems faced by the current big data field, and at the same time avoid the existing centralization problems [10]. The World Economic Forum report pointed out that there are currently more than 20 countries investing in blockchain-related technology areas, 80% of banks began to implement some blockchain distributed ledger-related projects in 2017, and the blockchain has become the Internet A technology that has received much attention around the world [11]. From the perspective of development trend, with the continuous maturity of blockchain technology and the increasing investment in blockchain technology research in hot industries around the world, people will explore the practical application of this technology in three stages [12]. Phase 1.0: Blockchain technology is mainly used to support digital currency represented by Bitcoin. By supporting transaction transactions such as transfer and payment between accounts, sellers and buyers can realize digital currency security without the help of third-party guarantees. Letter trading [13-15]. Phase 2.0: Combine digital currency with smart contracts, use blockchain technology to optimize a wider range of scenarios and processes in the financial sector, replace the contract with an algorithmic trading program, and trigger the network to automatically execute the contract through external conditions. In the financial industry, products such as bonds and derivatives are supported in asset trading, fund clearing, and intelligent agreements [16-19]. Stage 3.0: Blockchain technology extends from the economic field to social management, charity, culture and entertainment, medical health, science and culture and other social fields, challenging traditional centralized IT application systems, and may change our production in the future. , life and social rules [20]. The block chain was first proposed by Nakamoto in 2008 and became known and familiar with the popularity of digital currencies such as Bit coin [21]. In recent years, blockchain technology and application have attracted extensive attention in academia and industry in China. Major technology companies represented by BAT and financial institutions such as banks have carried out related technical research and application research and development. In July 2016, Alibaba's Ant Financial Service developed a blockchain-based donation platform. In September 2016, Tencent's Weizhong Bank first launched the bank blockchain business in China. In July 2017, Baidu launched Commercial-grade blockchain cloud application platform and more. Blockchain has a very broad application prospect in many fields such as Internet of Things,

financial technology, digital forensics, and e-government [22]. However, the blockchain technology was first proposed in 2008, and its theoretical research and application in various fields are still not mature and reliable. In the future, more new technology research and development is needed to further expand the usability and reliability of the blockchain. Many scholars have made efforts and contributions. Herlihy M et al. proposed a distributed computing platform based

on blockchain, which uses external blockchain as a network controller to implement access control and privacy protection [23]. In the same year, Aniello L, Baldoni R, Gaetani E and others proposed a distributed personal data management system based on blockchain, which enables users to better control their own data and achieve privacy protection [24]. Kiayias et al. proposed the first blockchain protocol based on the verifiable security-based equity proof mechanism, and compared the corresponding security attributes in the Bitcoin blockchain protocol [25, 26]. In this paper, the distributed agent model is deployed in the cloud by using the mobile agent technology. The virtual machine agent enables multi-tenants to cooperate with each other to ensure data trust verification, and complete the tasks of reliable data storage, monitoring and verification through the virtual machine agent mechanism. This is also a necessary condition for building a blockchain integrity protection mechanism. The blockchain-based integrity protection framework is built by the virtual machine proxy model, and the unique hash hash value corresponding to the file generated by the Merkel hash tree is used to monitor the data change by means of the smart contract on the blockchain, and the data is owned in time. The user issues a warning message for data tampering; in addition, a "block-and-response" mode is used to construct a blockchain-based cloud data integrity verification scheme.Cloud storage provides elastic storage services for enterprises and individuals remotely. However, security problems such as data integrity are becoming a major obstacle. Recently, blockchain-based verification approaches have been extensively studied to get rid of a centralized third-party auditor. Most of these schemes suffer from poor scalability and low search efficiency and even fail to support data dynamic update operations on blockchain, which limits their large-scale and practical applications. In this work, we propose a blockchain-based dynamic data integrity verification scheme for cloud storage with T-Merkle hash tree. A decentralized scheme is proposed to eliminate the restrictions of previous centralized schemes. The data tags are generated by the technique of ZSS short signature and stored on blockchain. An improved verification method is designed to check the integrity of cloud data by transferring computation from a verifier to cloud server and blockchain. Furthermore, a storage structure

called T-Merkle hash tree which is built based on T-tree and Merkle hash tree is designed to improve storage utilization of blockchain and support binary search on chain. Moreover, we achieve efficient and secure dynamic update operations on blockchain by an append-only manner. Besides, we extend our scheme to support batch verification to handle massive tasks simultaneously; thus, the efficiency is improved and communication cost is reduced. Finally, we implemented a prototype system based on Hyperledger Fabric to validate our scheme. Security analysis and performance studies show that the proposed scheme is secure and efficient. Nowadays, more and more companies have built their cloud computing services and open them to individuals or other enterprises, for instance, Amazon, Alibaba, Tencent, and Microsoft. As an important service of cloud computing, cloud storage allows clients remotely to store their data in cloud. By data outsourcing, clients enjoy many benefits, such as relieving themselves of heavy storage management, unlimited access at any time and any place, reducing expenditure on hardware/software, and employee maintenances. However, storing data in cloud makes clients lose local control over their data, which may cause potential security risk. One big problem is how to make sure that the integrity of outsourced data is intact. As we know, data loss or corruption with cloud servers often occurs due to malicious attacks, hardware failures, insider attacks, and even human mistakes [1–3]. Public verification has been extensively studied to verify the integrity of cloud data in recent years. A third-party auditor (TPA) is introduced to verify data integrity on behalf of clients periodically without local copies. The key ideal is that each data block is attached with a tag or signature, and the integrity verification depends on the correctness of these tags or signatures. During verification, the TPA sends a query with some random sampled data blocks to cloud server and then the cloud server calculates the proofs using the queried data and tags stored on it and respond them to the TPA. Finally, the TPA checks these proofs to judge the integrity of cloud data. The benefits and basic requirements of public verification in cloud storage have been discussed in previous scenarios [4, 5]. However, public verification is still subject to a series of restrictions. First, the assumption of complete trust on TPA is impractical because centralized TPA is more vulnerable to internal and external security threats from the Internet. Second, the TPA may cheat clients for profits by conspiring with cloud server to generate fake verification results. Third, when the received tasks exceed its processing capacity, the TPA has to delay the completion of previously agreed tasks. Therefore, the TPA cannot be absolutely trusted and may turn into a bottleneck of the system [6, 7]. Fortunately, blockchain technology provides a new perspective to dispose of

the above problems for the properties of decentralized data storage, point-to-point transmission, consensus mechanism, and encryption

[8]. Nevertheless, designing a decentralized verification scheme based on blockchain without TPA is a great challenge. If blockchain is used to store clients‘ data, the data tags or

signatures are not required [9]. It may limit its extensive applications because the structure of blockchain has a major obstacle in terms of capacity and scalability. Besides, it is not convenient for future data access and sharing. To overcome this drawback, Wang et al. [10] proposed a private PDP scheme to check remote data integrity by using blockchain technology. They used blockchain to store data tags while data files are still stored in cloud. However, their scheme should iterate through blockchain to obtain the challenged tags during verification, which is inefficient and impractical when blockchain grows large. Another major concern is that data dynamic operations have not been supported in previous blockchainbased schemes. Clients may not only access but also need to update cloud data, e.g., data modification, deletion, and insertion. Unfortunately, blockchain-based verification schemes mainly pay attention on static data files. Because blockchain is tamper-proof, a block cannot be modified once it is formed. This seems to make data dynamic operations difficult to implement. Thus, how to achieve blockchain-based data integrity verification and support data dynamic operations is necessary and valuable, which needs further exploration. In consideration of the key points of integrity verification and data dynamics for large-scale cloud storage, we propose a decentralized and dynamic integrity verification scheme with blockchain to check data integrity without requiring TPA and support fast retrieval. The main contributions can be summarized as follows. First, we present a decentralized cloud storage verification framework. Our scheme uses blockchain to overcome the obstacles brought by TPA and enhances the reliability of verification result. Data tags are calculated by the technique of ZSS short signature [11], and a new verification method is proposed to improve efficiency by transferring computation from a verifier to cloud server and blockchain. Second, to reduce storage overhead and improve search efficiency of blockchain, we propose a new storage structure called T-Merkle hash tree which is built based on T-tree and Merkle hash tree and design its search algorithm. Third, we extend the proposed scheme to support data dynamic operations, which is not considered by most existing blockchain-based schemes. In addition, our scheme achieves batch verification, which can handle massive verification tasks from different clients or for different data files at once. Fourth, we validate the correctness and performance of our scheme by implementing a

prototype system. Detailed security deduction shows that our scheme is secure, and experiment results demonstrate the efficiency of our scheme.

3. DISCUSSION

After running the suggested code through the Real-or-Random (ROR) model and the well-known Burrows-Abadi Needham (BAN) logic, we can see that it is safe. The proposed framework outperforms the current schemes in terms of security features, computing costs, and communication costs after a thorough comparison with existing competing schemes, including the studied system. Ensuring that privacy-protecting security measures that use blockchain technology do not negatively impact the digital twin environment's operation and efficacy is the purpose of the proposed approach. Reducing processing cost, improving algorithms, and striking a balance between security and efficiency are all possible steps in this direction. The suggested system's benefits Improvements to Data Security Transactions that are both transparent and immutable Trustlessness and decentralization Automating Smart Contracts: Enhanced Safety. There are three parts to this project: 1. Owner of Data 2. User of Data 3. Server in the Cloud 4. First Network 5. Second Network Renderer of Data

• Fill out the account registration form with the necessary details ou can:

• Request a key after being permitted to do so by the cloud owner

• Log in to your account

• If necessary, choose the network and node for the uploaded file, and see the key before uploading it in an encrypted manner.

• See documents • Sign in with your primary details

• Log out of your datauser account

You may access your uploaded files in an encrypted format once you've been approved by the cloud. You can also request a specific file and, if you input the key properly, it should be downloaded. • Make sure it is in decrypted format after downloading.

Exit from the cloud server. Make sure you're logged into the account with the right credentials. Then, go head and approve the owner. • View users and grant them permission.

You can see the owner's request and the key they sent for file upload, as well as all the files that were uploaded, see the graph, log out of NETWORK1, log in with the correct credentials, view the files that were uploaded to NETWORK1, log out of NETWORK2, log in with the correct credentials, view the files that were uploaded to NETWORK2, and log out of NETWORK1.

4. RESULTS

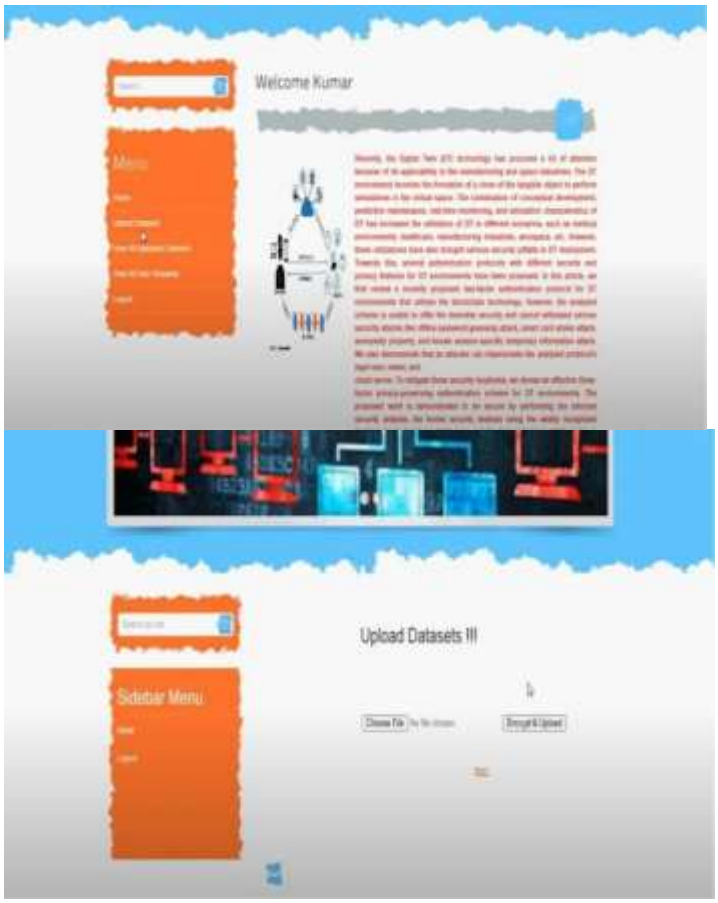
HOME PAGE

CLOUD LOGIN

BLOCK CHAIN LOGIN PAGE

DATA OWNER LOGIN PAGE

DATA OWNER PAGE



Pass Valid Credentials and enter in to data owner

page **UPLOAD DATA SET**

In Data Owner Page Upload Data Set By clicking Choose File The Data will Be Decrypted and uploaded to server

VIEW DATA PAGE

We are Displaying Data set Which We Uploaded in cloud server page

DISPLAYING ALL TEXT DATA SETS BY LOCATION BLOCK CHAIN

5. CONCLUSION

We looked into the scheme's proposed weaknesses and design issues in relation to several cryptographic attacks, such as offline password guessing, KSSTIA, and user impersonation. An improved three-factor-based privacy-preserving authentication architecture was suggested for the DT environment using blockchain technology. The suggested approach is efficient and more secure against several malicious assaults, according to the informal security study. Also, we'd want to build a full testbed experiment to see how the suggested approach works in practice.

6. REFERENCES AND CITATION:

[1] B.Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino, __Materials, structures, mechanical systems, and manufacturing roadmap,“ NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.

[2] H. Laaki, Y. Miche, and K. Tammi, __Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,“ IEEE Access, vol. 7, pp. 20325–20336, 2019.

[3] H. Wang and J. Zhang, __Blockchain based data integrity verification for large-scale IoT data,“ IEEE Access, vol. 7, pp. 164996–165006, 2019.

[4] C.Nagarajan and M.Madheswaran - ‗Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[5] C.Nagarajan and M.Madheswaran - ‗Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[6] C.Nagarajan and M.Madheswaran - ‗Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[7] C.Nagarajan and M.Madheswaran - ‗Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[8] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. ―Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter‖ Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[9] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya ―Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay‖ Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[10] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash ―Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM‖ Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[11] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable undesirable emergent behavior in complex systems" in Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches, Cham, Switzerland:Springer, pp. 85-113, 2017.

[12] B. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart and A. Calomino, "Materials structures mechanical systems and manufacturing roadmap", 2012.