Advanced Security Model for Multimedia Data Sharing in Internet of Things

Dhar, Shalini; Khare, Ashish; Singh, Rajani

Document Version
Final published version

Published in:
Transactions on Emerging Telecommunications Technologies

DOI:
10.1002/ett.4621

Publication date:
2023

Citation for published version (APA):
Dhar, S., Khare, A., & Singh, R. (2023). Advanced Security Model for Multimedia Data Sharing in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *34*(11), Article e4621. https://doi.org/10.1002/ett.4621

Received: 5 April 2022 | Revised: 21 June 2022 | Accepted: 18 July 2022

DOI: 10.1002/ett.4621

SPECIAL ISSUE ARTICLE

WILEY

Advanced security model for multimedia data sharing in Internet of Things

Shalini Dhar[1] | **Ashish Khare**[1] | **Rajani Singh**[2]

[1]Department of Electronics and Communication, University of Allahabad, Prayagraj, India

[2]Centre for Business Data Analytics, Department of Digitalization, Copenhagen Business School, Frederiksberg, Denmark

Correspondence to:
Rajani Singh, Centre for Business Data Analytics, Department of Digitalization, Copenhagen Business School, Frederiksberg, Denmark.
Email: rs.digi@cbs.dk

Funding information
University Grant Commission

Abstract

Sharing a file that contains multimedia data among the different peers of wireless Internet of Things (IoT) networks has several challenges. One of the main challenges is their centralized system, which leads to high-security risk and low user reachability. One solution could be to simply change the system to a decentralized network by using the blockchain network to store these files. However, it may solve the low user reachability and security problem at the cost of low latency, longer response time, scalability and privacy issues. Therefore, this article uses the advanced blockchain scheme and distributes InterPlanetary File System. We also presented the system framework and its working. Finally, we do the security analysis of our proposed system and found that it has strong potential to solve most of the security challenges that traditional system faces. Moreover, our proposed approach can be applied to any file-changing wireless IoT network that needs to exchange multimedia data such as healthcare data, IoT data in wearable devices, traffic data in smart cities, etc.

1 | INTRODUCTION

Multimedia is a medium that allows information to be easily transferred from one location to another.[1] It is an interactive media and provides multiple ways to represent information to the user in a powerful manner. It provides interaction between users and digital information. It is a medium of communication. Some sectors where multimedia is used extensively are education, training, reference material, business presentations, advertising and documentaries. Multimedia, as the name suggests, is the combination of multi and media that is many types of media (hardware/software) used to communicate information.

Multimedia presents text, pictures, audio, and video with links and tools that allow users to navigate, engage, create, and communicate using a computer. It refers to the computer-assisted integration of text, drawings, still and moving images (videos), graphics, audio, animation, and any other media in which any type of information can be expressed, stored, communicated, and processed digitally.[2] To begin, a computer must be present to coordinate what you see and hear and interact with. Second, there must be interconnections between the various pieces of information. Third, you will need navigational tools to get around the web of interconnected data. Multimedia is employed in various disciplines, including education, training, and business.

By definition, multimedia is a representation of information attractively and interactively with a combination of text, audio, video, graphics, and animation. In other words, we can say that multimedia is a computerized method of presenting information combining textual data, audio, visuals (video), graphics, and animations. Example: E-mail, Yahoo messenger, video conferencing, and multimedia message service. Multimedia data security is a form of content-based protection. It is the practice of protecting the user's digital information from unauthorized access, tampering, corruption, or theft throughout its entire lifecycle. It is a protective measure that keeps unauthorized access away from databases, websites and computers. Therefore, it provides a mechanism for protecting multimedia data from loss or corruption.

Multimedia data security addresses the problems of digital watermarking, digital rights management, data encryption, multimedia authentication, etc. So, it covers every aspect of information security: from physical security to administrative and access controls, as well as the logical security of software applications. Here by physical security, we mean security of hardware and storage devices, and by logical security, we mean protection of the software applications. There are different type of multimedia data security solutions available. Most popular solutions are as given below:

- *Encryption*: In encryption techniques, different cryptographic algorithms are being used to transform normal or plain text characters into an unreadable format called cipher text. Encryption keys are used to decode the multimedia data from cipher text to plain text so that the authenticated users can only access the data. The vast majority of solutions uses such security key management capabilities. However, it is not suitable for sharing multimedia data in Internet of Things (IoT) networks as the data needs to process fast and among several users. So, key exchange will be very challenging and time taking.
- *Data erasure*: Data erasure is a software-based method used to overwrite multimedia data on any storage device completely. Although it is more secure than standard data wiping, such data is unrecoverable. it is also not suitable for exchanging multimedia data in IoT networks as the deleted data can be needed later on by the other nodes or peers.
- *Data masking*: Data masking is a method to create a fake but realistic version of organizational multimedia data. It is used to protect sensitive data while providing a functional alternative in a case when real data is not needed. In this process, data values are changed using the same format. For example in user training, software testing or sales demos. It is important to note that masked multimedia data cannot be deciphered or reversed. Data masking can be done in various ways, such as altering the data, word or character substitution, including character shuffling and encryption. However, it does not work in IoT networks because of the same reason as mentioned above in encryption.
- *Data resiliency*: Resiliency is determined by how well an organization recovers from any type of failure. Failure could be anything from hardware problems to power shortages and other events that affect multimedia data availability. The term "data resiliency" refers to data's ability to "spring back" in situations where it is compromised. Speed of recovery is critical to minimize impact. It is very important that the multimedia data is always available to its users. Therefore, it is essentially an organization's ability to avoid unexpected disruptions to data workflows.

IoT is a network of physical objects such as devices, vehicles, wearables, buildings, offices, etc., embedded with sensors, electronics, software, processing ability, and network connectivity or other technologies that allow the exchange of data between other devices. Data are generally in huge volume.[3] So data exchange between other devices and systems is done over the communications networks either through wired or wireless means.

The most popular way is exchanging data over the Internet. IoT structure consists of three main things: sensors, a gateway device, and the cloud server. Communication in IoT takes place over the cloud server, and all the communicating devices will have to use the same Internet protocol (IP).[4]

Communication establishes through the gateway device in either wide area network (WAN) mode or in Ethernet mode. Sensors are connected to the gateway device and deployed at the remote location to detect any changes in the environment and notify the system used for the occurred changes. These changes are then captured and pushed to the cloud server. There are mainly four types of communications in IoT[5] given as follows:

1. *Human to machine*: It is a combination of software and hardware that includes human interaction with a machine to perform a task, for example, facial recognition.
2. *Machine to machine*: In this, communication takes place between machines by automating data/programs. It is a point-to-point connection between two network devices that helps transmit information using public networking technologies like Ethernet and cellular networks.
3. *Machine to human*: It is a way of interaction in which humans co-work with smart systems and other machines by using tools or devices to finish a task, such as traffic lights, fitness bands, health monitoring devices, fire alarms, etc. This type of communication is most commonly used when machines guide humans in their daily life.

4. *Human to human*: This concerns how humans communicate with each other to exchange information by writing, speech, drawing, body language, facial expressions, etc. Machine to machine applications cannot produce the expected benefits unless humans can immediately communicate to solve challenges, fix issues, and manage scenarios. For instance, many protocols are used in the communication of IoT devices. These IoT protocols are modes of communication that give security to the data being exchanged between IoT-connected devices such as Bluetooth, Wi-Fi, etc.

The Internet of Multimedia Things (IoMT) is the collection of interfaces, protocols, and associated multimedia-related information representation that enable advanced services and applications based on the device to device and human-to-device interaction in virtual and physical environments. IoMT devices differ from IoT devices as they require higher computational power, bigger memory, and more power-hungry with higher bandwidth. It also generates a massive volume of data with different characteristics and requirements than the IoT. Wireless networks[6] exist almost everywhere people work or live, but "what is a wireless network" and "how they work" are often enigmatic concepts. So, first, we try to unfold these riddles (Figure 1).

Wireless networks are computer networks[7] that use radio frequency or radio waves to establish connections between nodes or devices. Wireless networks are a cost-effective solution for businesses, homes, and telecommunications networks because they do not use any kind of cables to connect their various nodes in the network.

Let's take the example of the Wi-Fi hot spots in public places such as cafés, shopping malls, etc. If you open the Wi-Fi of your mobile device, iPad, or laptop and connect to that particular Wi-Fi hot spot, the internet connection is established to that cafe's or shopping mall's wireless network.

People often get befuddled and assume that all wireless network is Wi-Fi as they both use radio waves, but they are not synonymous. It is essential to know that there are many different types of wireless networks across various technologies, such as LTE, 5G, Bluetooth, and ZigBee. On the other hand, Wi-Fi is a wireless protocol defined by the Institute of Electrical and Electronics Engineers (IEEE) in the 802.11 specifications and its amendments.[7,8]

There are four main types of wireless networks or connections:

- Personal area network: A network centralized around the devices of a single person in a single location.
- Interconnect nodes or devices in a short-range or area such as within a person's reach.
- Local area network: Connect two or more nodes or devices using a wireless distribution method, providing a connection through access points to the wider Internet.

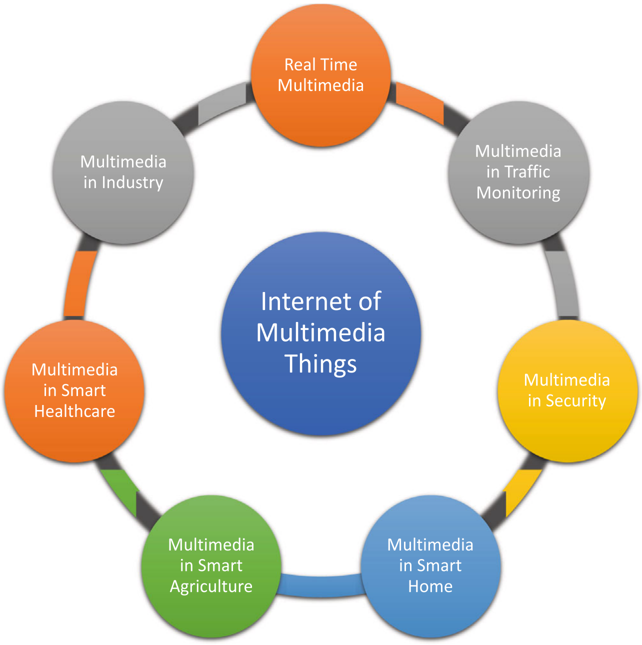

Real Time Multimedia
Multimedia in Traffic Monitoring
Multimedia in Security
Multimedia in Smart Home
Multimedia in Smart Agriculture
Multimedia in Smart Healthcare
Multimedia in Industry
Internet of Multimedia Things

FIGURE 1 Application of Internet of Multimedia Things

- Metropolitan area networks: Connects several wireless LANs.
- Wide area network: Covers a broad range or area such as neighboring towns and cities.

In this article, we discuss and propose a framework for multimedia data sharing system that is secure against several widespread security attacks such as eavesdropping, distributed denial of service, message tampering, man in the middle attack, data leakage, etc. Our model also used the strongly secure authentication protocol based on zero-knowledge proofs, guaranteeing multimedia data user privacy. Our proposed multimedia data file sharing system can be applied in several areas, and some of them are listed below:

- *Healthcare*: Majority of the healthcare data are in the form of multimedia data such as heart rate reading, electrocardiogram or ECG, computerized tomography (CT) scan, etc. Therefore, our proposed system framework can be used to exchange these healthcare data over wireless networks.
- *Smart home*: For security reasons, people use security or CCTV cameras in their smart home, which they can access from anywhere in the world. So, ultimately they are exchanging these audio videos over the internet. If several family members want to access this data or share it with the security company, it will be possible by using our system framework. Also, the unauthenticated user will not be able to access these data.
- *Transportation*: In the smart city, smooth traffic transportation requires quick data exchange such as current traffic situation, busy roads, if there is any traffic jam, etc. All these data are multimedia data. So our proposed model fits well here.
- *Industry*: Several industries contain confidential and sensitive information in the form of multimedia data. These data could be contact details with the demo (video or PowerPoint), audio or video if we think about the music industry or combined text, audio, and video if we think about the news industry. With our proposed system, exchanging these multimedia data among the industry employee can be done securely.

2 | LITERATURE REVIEW

IoT is becoming the emerging technology paradigm surrounded by heterogeneous technologies comprising smart ubiquitous objects connected to the common Internet. These IoT devices were deployed often in the open-based environment to offer innovative services in several application domains, including smart communities, smart health, and smart cities, industry.[9] These IoT devices generate a huge volume of security-sensitive and confidential information. For this purpose, some studies illustrated the implementation of decentralized access-control and authentication procedures for handling lightweight IoT devices.[10] Research in IoT by using data mining,[11,12] its privacy preserving issue[13,14] has got sufficient attention.

These IoT devices relied on public blockchain concepts and may be based on fog computing. These systems exhibit higher performance levels than other blockchain-based authentication process. A new decentralized architecture design[15] is modeled upon the basis of a blockchain network for ad-hoc nodes and flying nodes.[16] The blockchain network is well-defined for decentralized features, which can be utilized for centralization issues in flying ad hoc networks. Practical Byzantine fault tolerance is employed for maintaining consensus between nodes. This design makes efficient and faster architecture for the blockchain network.

An extensive and very informative literature review on applications of wireless sensor networks and IoT frameworks in the Industry Revolution 4.0 can be found in Reference 17.

The IoT and artificial intelligence (AI) integration with blockchain technology play predominant roles in healthcare streams and agriculture fields to manage product traceability, food supply-chains, intelligent-predictions systems, connected devices, product monitoring processes, smart contracts, and drug supply-chains.[18]

In Table 1, we present the comparison of existing literature and related work with the system framework proposed in our article.

Blockchain technology aids to build a secure and transparent system wherein relying on IoT devices turns out applications as flexible, efficient infrastructure and connected system. The combination of these technologies highly impacted healthcare industries. IoT framework consists of a physical objects network comprised of embedded technology for communication, sensing and internal-state interaction, or external environment interaction. In this decade, several healthcare systems and their solutions are achieved by design with IoT technology.[26] But the complexity of this phenomenon is they

TABLE 1 Comparison of existing literature with the proposed framework

Author	Description	Year	Limitations
Kumar et al[19]	Describe a lightweight cryptography method for IoT at perception layer.	2020	No device authentication, key management, identity management, and access management.
Khattak et al[20]	Article discussed about attacks and security challenges such as sensor network or RFID attacks.	2019	Lack of key management and device authentication.
Dwivedi et al[21]	Article discussed privacy challenges of blockchain-based medical system and solved the privacy issues using non-interactive zero knowledge based cryptosystem.	2021	Lack of device authentication, two-factor authentication, identity management, and access management.
Lucia et al[22]	Article discussed about authentication mechanism at perception layer for smart home applications.	2019	Lack of key management, lightweight cryptography, and two-factor authentication.
Wu et al[23]	Article discussed security and privacy challenges of blockchain-based medical system. Authors used cryptographic algorithms to secure the system.	2014	No device authentication, identity management, and access management.
Singh et al[24]	Article discussed security challenges and solutions of IoT based pharmaceutical supply chain management system. Also solved the issues using key management and trust management techniques.	2014	Lack of device authentication, two-factor authentication, and privileged access management.
Jing et al[25]	Article discussed security challenges of IoT system. Also solved the issues using key management and trust management techniques.	2014	No device authentication and privileged access management.
This article	This study employed a secure, privacy-preserving and fast decentralized device-to-device file-sharing system model utilizing a blockchain network over the wireless Internet of Things.	2022	We tried to remove the above issues from this work and proposed a new blockchain and IPFS-based multimedia file sharing system with high latency.

would possess centralized database access. Hence there occurs the risk of insecurity in data access, and the organization might demand charges for secure storage. By utilizing this blockchain technology, these issues would be addressed. This applies to distributed and decentralized database storage systems where the data could not be shared without approval from either side.

Focusing on this implementation, the Internet of Medical Things defines as the medical devices and medical-application collection, which is interconnected to health-care-IT systems.[27] This would facilitate the patients in avoiding manually carrying reports during each visit; rather, it is present in the blockchain network. Along with blockchain, the cryptography utilization scheme on the basis of asymmetric-cryptographic and symmetric-keys was recommended in IoT infrastructure because it could not handle energy-containment, storage process, and handling method.[28] Hence, blockchain is formulated to deal with security issues within IoT in the problems mentioned earlier. Similarly, the analytic hierarchy process based on the intelligent-decision-making technique is employed for maintaining concurrent, interoperable and secure systems in IoT devices.[29]

This healthcare industry is focused on and exhibited how this can be facilitated from distributed-ledger-technology (DLT) and blockchain for automation-process, smart contracts, access-control, and electronic medical record management.[30] The present innovations of the healthcare stream are examined by blockchain technology as a platform basis. A broader healthcare data-protection technique is concentrated upon DLT. This technique seems to be the distributed secure application defined as Healthify. In this DLT, the medical information is made encoded to offer a secure environment. The secure healthcare information was delivered with distributed application architecture within the operational medical system.[31] A distributed system based on health-information exchange upon a blockchain network is proposed for this remedy. This framework is utilized for healthcare aspects, including insurance claim enhancement and promoting information made available for research firms. Some of these conventional e-health-care systems relied on a single blockchain[32] network system through a unified system. This converted information process and information synchronization process is employed for larger-scale e-health information to make the inefficient system migration, access-control mechanisms, and data storage.[33]

The blockchain network could enhance the scalability of data and partition network with the help of a consensus algorithm to contest COVID-19.[34] Multi-drone tasks perform this through detection and monitoring, collision avoidance, data analysis, goods delivery and medical supply, sanitization and social distancing. In this study, end-to-end application delivery is achieved by integrating multi-drone tasks and blockchain network architecture to combat COVID.[35] The m-health-framework is organized with IoT technologies and a blockchain network to aid patients upon their diagnosis and treatment phases to maximize patients' involvement. Similarly, the blockchain framework, along with IoT technologies, aids in remote patient monitoring, cost minimization, diagnosis detection, and unnecessarily hospital visits.[36] Likewise, to combat the COVID crisis, the multi-robot decentralization through blockchain network and management played a significant role in minimizing goods-delivery, monitoring process and in reduction of human interaction.[37] The blockchain approach does managing multi-robot collaboration and enhances the interactions for efficient information exchange, goals-sharing, trust-factor and sharing representation. The existing cloud-basis information sharing platform does have privacy and security complications.[38]

The trusted AI models upon blockchain networks are explored for content-based information sharing systems for the e-health-care system. The data traceability and data sources utilized for AI-model building and AI-model training in distributed data-stores.[39] The smart-contract and blockchain network is depicted as security remedies for the IoT framework. The blockchain network enables decentralized access-control, defined as BlendC-access control. This access-control mechanism rectifies the issues pointing to the low rate of the transaction and a high level of data storage from the blockchain framework.[40] The traditional rock, paper, scissors, and hammer game is enhanced by utilizing cross-chain simulation and blockchain networks to check out data transactions securely, and messages during the game.[41] The interface for this communication is enabled for safety interaction through smart contracts and blockchain networks. This smart-contract utilization and decentralization are analyzed by proposing the novel architecture IoMT for e-health-care information. This model, the dimensions of the decentralization process.[42]

In the healthcare field, specifically in accidental use, the role of the blockchain network is immense such that it evolves the new model distributed ledger-based IoT-framework is employed.[43] This framework consists of a hyperledger-sawtooth blockchain with an InterPlanetary File System (IPFS) depicted as distributed storage. In this model, the cars transmit data to respective smart-contract. Lightweight elliptic-curve Qu-Vanstone with multi-access edge computing (MEC) and blockchain architecture is employed in the medicinal field for data authentication, integrity, and data privacy among IoT cloud and MEC authentication. Smart-contract handles access-control mechanisms.[44] The present trend in data communication is the blockchain based-approach for authentication. This blockchain network could leverage to offer transparent data communication,[45-47] such that these data permit the secure level of recording in a wider diversified hospital network.[48] Similarly, decoupled blockchain network is presented within the edge-envisioned ecosystem. The technique leveraged neighboring edge devices to generate decoupled blocks for secure healthcare data transmission from sensor point to Edge-notes.[49]

The blockchain demands, specifically in the healthcare system, are enormous. It obtains the activity of intermediates, patient data records or shipment process moving IoT objects from provider place to users place, and it is also decentralized.[50,51] In a machine-learning platform, this blockchain system aids in determining medical datasets and intrusion attacks. In this stage, this decentralized solution with IPFS storage was used for confidentiality in many entities.[52] Another study that decentralized state architecture in e-health consists of three main layers. Such as the sensing-layer with medical sensors in the patient's body to mobile, NEAR-processing layer, consisting of edge-networks and FAR-processing-layer with higher computing-servers or clouds.[53] In fog-computing, there were poisoning attacks, congestion in the network, and latency.

The utilization of a blockchain system enabled federated-learning is employed to rectify these issues. This FL-process enabled decentralized privacy-prevention through access-control, off-chain data retrieval, and storage to control single-point data failures.[54] The resource-constrained IoT based benefits can be combined with blockchain lightweight-network (BLWN) to do materialization of all applications within e-health-care.[55] This encounters the aspects of e-health care application within IoT-orientation. Altogether the IoT environment and present cloud-computing technology are leveraged to generate telemedical services, such that patients are made to co-operate for clinical examinations carried down by technicians by using IoT devices.[56] The outcomes were transmitted automatically to doctors through hospital-cloud servers for further treatment or consultation.

3 | COMPONENT OF SYSTEM ARCHITECTURE

3.1 | Blockchain

One of the essential structures of our system architecture is blockchain. It is a distributed data ledger that is immutable. Unlike in centralized network systems in the blockchain system, nodes of a computer network are connected in a decentralized manner.

The blockchain database has a different data structure and relies on the Merkle hash tree. All transactions broadcasted from the other peers or nodes are collected and grouped in bundles, kept in blocks, and added to the chain. Since blocks have a specific storage limit, remaining transactions are automatically moved and stored into the new block once they are full. This new block also keeps the previous block's hash value and is then added to the chain. Blocks also contain the timestamp, which tells when the block is added to the chain. This process continues, making a chain of several blocks; that is why it is called the blockchain. The transactions in blocks are immutable, meaning that once they are added to the blockchain, an adversary cannot change or tamper with the data (Figure 2).

Blockchain has three important properties described as follows:

- *Scalability*: Blockchain is scalable compared to the traditional data structure. Each block can contain a set of transactions of a specific size limit. Because of its scalable property, we used it for sharing and exchanging multimedia data. More research to improve scalability is already an ongoing area.
- *Tamper-proof*: Distributed ledger of blockchain is tamperproof, which means that it is impossible to change or manipulate the data once it is stored as a transaction in the blockchain. This property ensures that the multimedia data are not modified while exchanging or sharing the data among different peers.
- *Security*: Blockchain is strongly secure as it relies on secure and complex mining schemes such as proof-of-work or proof of stake, to name a few. Blockchain security also guarantees the safety of multimedia content stored in its block.
- *Decentralized*: Centralized systems always have drawbacks, especially when the peer or nodes do not trust each other. However, blockchain is a decentralized system that builds trust among its peers or nodes. Therefore, a decentralized blockchain system will also remove the mediator's need to exchange or share multimedia content.

3.2 | Hash function

Both input and output data values can be alphanumeric. A mathematical function that converts an input value or data of arbitrary length into output value or data of fixed length is called a hash function. The value returned by a hash function is called the message digest or hash value (Figure 3).

Popular Hash functions. Here are some popular hash functions with their relevant information. The hash function has the following essential properties:

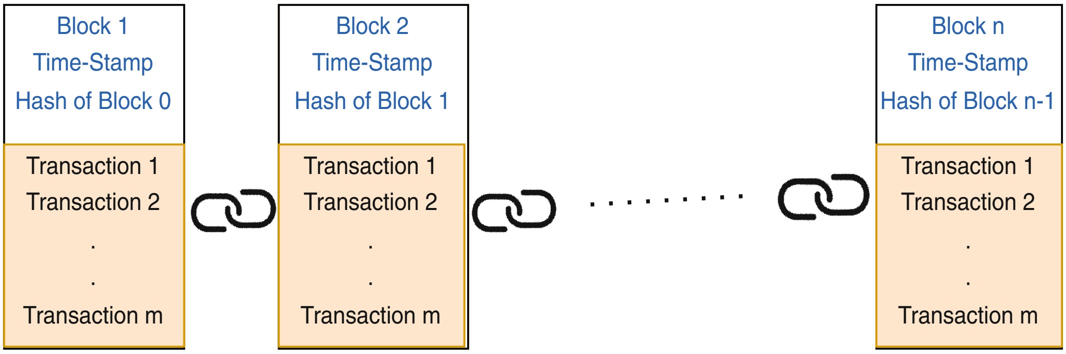
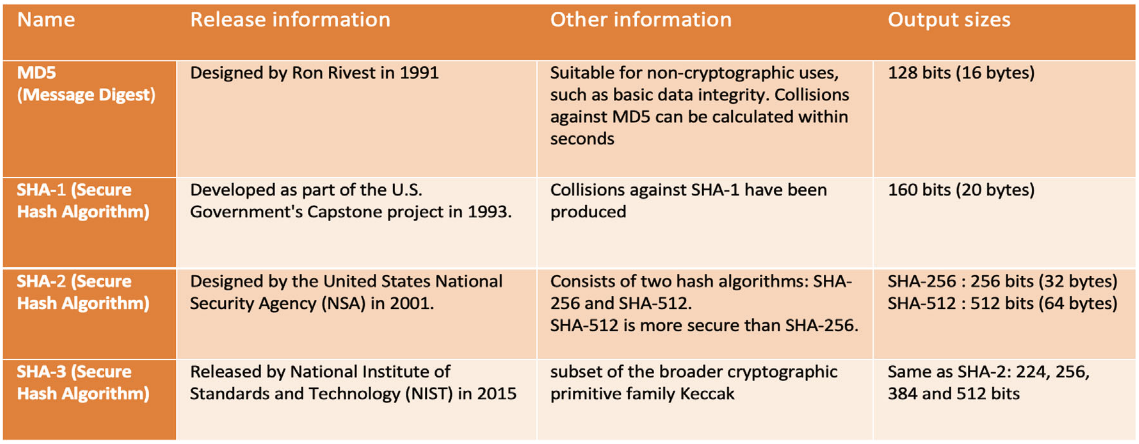


FIGURE 2 Blockchain data structure



Name	Release information	Other information	Output sizes
MD5 (Message Digest)	Designed by Ron Rivest in 1991	Suitable for non-cryptographic uses, such as basic data integrity. Collisions against MD5 can be calculated within seconds	128 bits (16 bytes)
SHA-1 (Secure Hash Algorithm)	Developed as part of the U.S. Government's Capstone project in 1993.	Collisions against SHA-1 have been produced	160 bits (20 bytes)
SHA-2 (Secure Hash Algorithm)	Designed by the United States National Security Agency (NSA) in 2001.	Consists of two hash algorithms: SHA-256 and SHA-512. SHA-512 is more secure than SHA-256.	SHA-256 : 256 bits (32 bytes) SHA-512 : 512 bits (64 bytes)
SHA-3 (Secure Hash Algorithm)	Released by National Institute of Standards and Technology (NIST) in 2015	subset of the broader cryptographic primitive family Keccak	Same as SHA-2: 224, 256, 384 and 512 bits

FIGURE 3 List of popular hash functions

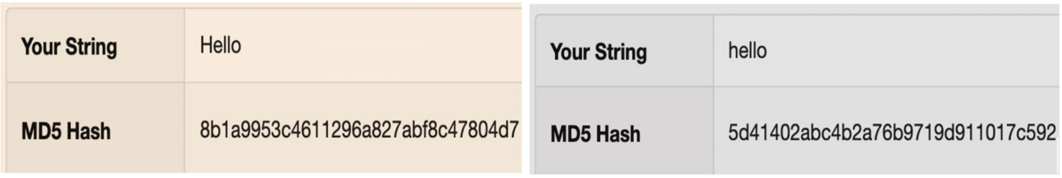
1. *Deterministic*: The hash function will return the same output hash value for the same input value. This characteristic of the hash function ensures the authenticity of data. Suppose a user requests a multimedia file named A with a particular hash value and receives a B file. The user applies the same hash function on both files A and B, and if both give the same hash value output, it guarantees the user that both files are the same.
2. *Unique*: It will be impossible to generate the same output hash value for two different input values. The hash functions should be designed so that they are strong collision resistance. In modern cryptography, collision resistance hash is considered the fundamental building block of data security.
3. *One-way*: It is not possible or computationally infeasible to guess the input values for a given output hash value. This property ensures that computing from one direction is straightforward; however, inverting or computing from another direction is extremely hard or almost impossible. So, it guarantees that the input data file is safe even if the adversary knows its hash output value. Brute-force attacks or rainbow tables attacks can breach the security in less secure hash functions.
4. *Uncorrelated*: A small change or modification in the input value will result in a different hash output value. It ensures that the adversary cannot tamper or change the file. And if it happens, it will be visible by matching the hash value. Here we generate a hash value for the string "Hello" and "hello" by using.[57]

In our IPFS system, we use the SHA2-256 algorithm to hash the multimedia content (Figure 4).

3.3 | Authentication

In order to increase the trust among the system users, the blockchain system needs to check the authenticity of the end-users. So, when someone requests the multimedia file from the blockchain system, it needs to check the identity of the user. For that, we are using the Schnorr identity protocol. As advancement and to reduce the cost of communication in the blockchain network, we use the non-interactive version of the Schnorr protocol.

The Schnorr identification protocol is proposed by C. Schnorr. It is based on the assumption that the discrete logarithm problem is hard or intractable and thus provides strong security against eavesdropping attacks.



Your String	Hello
MD5 Hash	8b1a9953c4611296a827abf8c47804d7

Your String	hello
MD5 Hash	5d41402abc4b2a76b9719d911017c592

FIGURE 4 Hash value for the same word

Definition 1 (Discrete log assumption). Let G be a cyclic group of order p and $g \in G$ generator. According to discrete log assumption, on the one hand, it is easy to compute the value of $A = g^x$ for $x \in G$. On the other hand, given A, it is infeasible or computationally very hard to guess the value of x. So, doing one-way computation is easy, but computing in the opposite direction is almost impossible.

In the Schnorr user identity protocol, this x is known as the secret key, and the corresponding public key can be defined as $T = g^x$.

Schnorr user identity authentication protocol. In this protocol, a prover named Peggy wants to prove her identity to a verifier named Victor. For that, Peggy has to convince Victor that she knows the secret key x without revealing the value itself. The interactive version of this identity authentication protocol is as follows (Figure 5):

- *Commitment*: First, Peggy computes a value $T = g^u$ by using the generator g and sends it to Victor.
- *Challenge*: Victor challenges Peggy by sending a numeric value c and ask her to find the solution s of that challenge. Note that this challenge value is chosen such that Peggy will not be able to find the solution until she knows the secret value. So, this will convince Victor that Peggy knows the secret value.

  So, Peggy computes the solution s for the given challenge c and sends back this proof of the secret key to Victor.
- *Verification*: Since Victor knows the value T, A, c, s. So, he will check if g^s is equal to $T.A^c$. If this is true, then Victor is convinced by Peggy's proof. As a result, Peggy's identity is successfully authenticated by Victor.

However, to reduce the communication cost and response time, we have proposed a non-interactive version. Instead of sending the challenge by Victor, it is now calculated by using the Hash function that is $c = \text{Hash}(g, A, T)$.

3.4 | Multimedia file IPFS

IPFS[58,59] is a decentralized system used for storing and sharing the files that contain multimedia data such as text, audio, video, image, etc. Using IPFS for data communication and exchange in the IoT provides strong security and low latency. IPFS utilizes the content-based addressing concept and defines how data in files moves over the IoT network and create a distributed file storage system. IPFS network is very efficient as it prevents file redundancy because of a unique hash-based address. When multiple peer nodes publish the same file on the IPFS network, the file will only be created once. When someone requests a file, they request that file directly by its hash ID instead of the actual file itself.

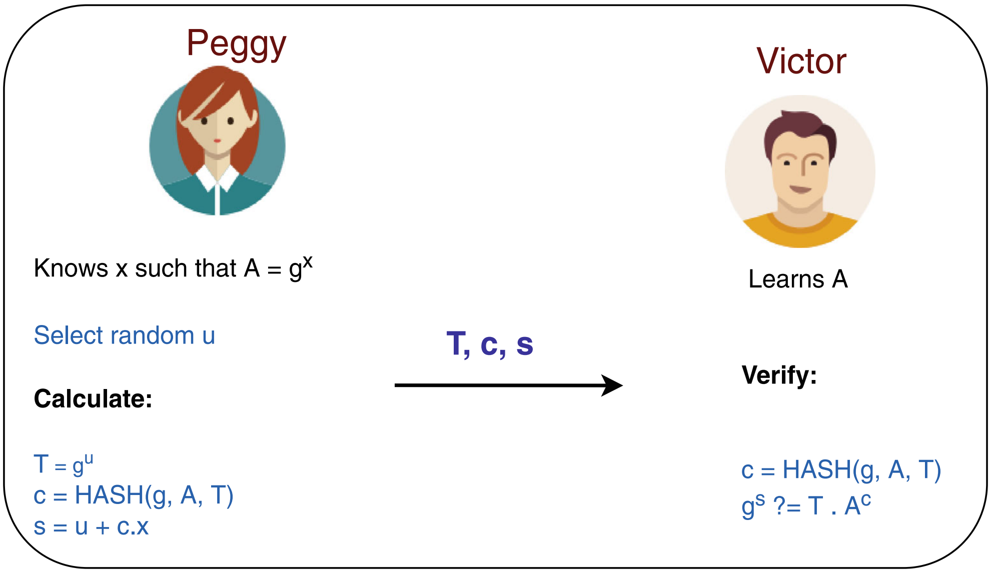


FIGURE 5 Schnorr user identity authentication protocol

Files up to 256 kB size can be stored as a single IPFS object. To store the larger file (image, video) in IPFS, it is broken up into smaller chunks of 256 kB called IPFS objects and spread across a network of nodes and computers. The IPFS system will then create an empty object that links to all the other chunks of the file. Generating a unique ID is based on the concept of the Merkle tree. Each chunk of the original file has given a hash ID which is then combined to generate a unique hash ID.[59] So, all files on IPFS are addressed by their unique hash ID. IPFS supports versioning of the files which means one can update the files while using the IPFS system (Figure 6).

Before discussing how the IPFS file-sharing or searching works, it is important to understand how we find or access any specific content or webpage from the Internet. Accessing or downloading any multimedia data that can be a photo, audio, or video from the Internet works on the location-based addressing technique. For example, suppose someone wants to download multimedia data from the Internet. In that case, it needs to tell the computer or system IP address or the domain of that data, which is the actual location of that multimedia data. So, a person's system needs to know where to find that particular data. However, the problem with location-based addressing is that one might not always get the data. The reason could be anyone; network traffic, data is not available anymore, original data has tampered, etc. Now let's discuss the working of IPFS based on content-based addressing. So in IPFS, the question changes from "where to find multimedia content?" to "what multimedia content do you want?"

In IPFS, every file has a unique hash that can be treated as the fingerprint of that file. So, to download or access a certain file, one needs to broadcast the hash query to the IoT network, asking who is the owner of that file with this hash? After receiving the hash request, the file owner of a particular hash on the IPFS network will send the file. Now an obvious question comes into mind: Can the file owner be trusted, or what if the file is tempered? The answer to this question is very simple. One needs to verify this by comparing the hash of both files requested and the received one. If the hash value of both files matches, that means that the file is secure and tamperproof.[60]

4 | SYSTEM FRAMEWORK AND WORKING

System Framework and its working is shown in Figure 7. System architecture working is divided into the following steps.

- *Step 1: User request*. In the first step, the user requests the file they want to access. In the example shown in Figure 7, the user wants to access and download the video file. This video file request of the user is then sent directly to the blockchain network.

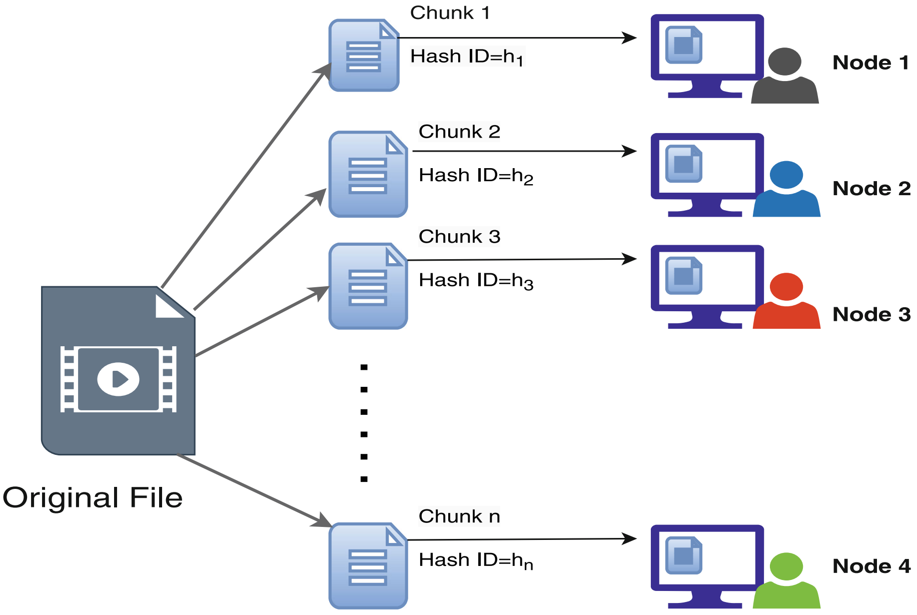


FIGURE 6 Storage in IPFS

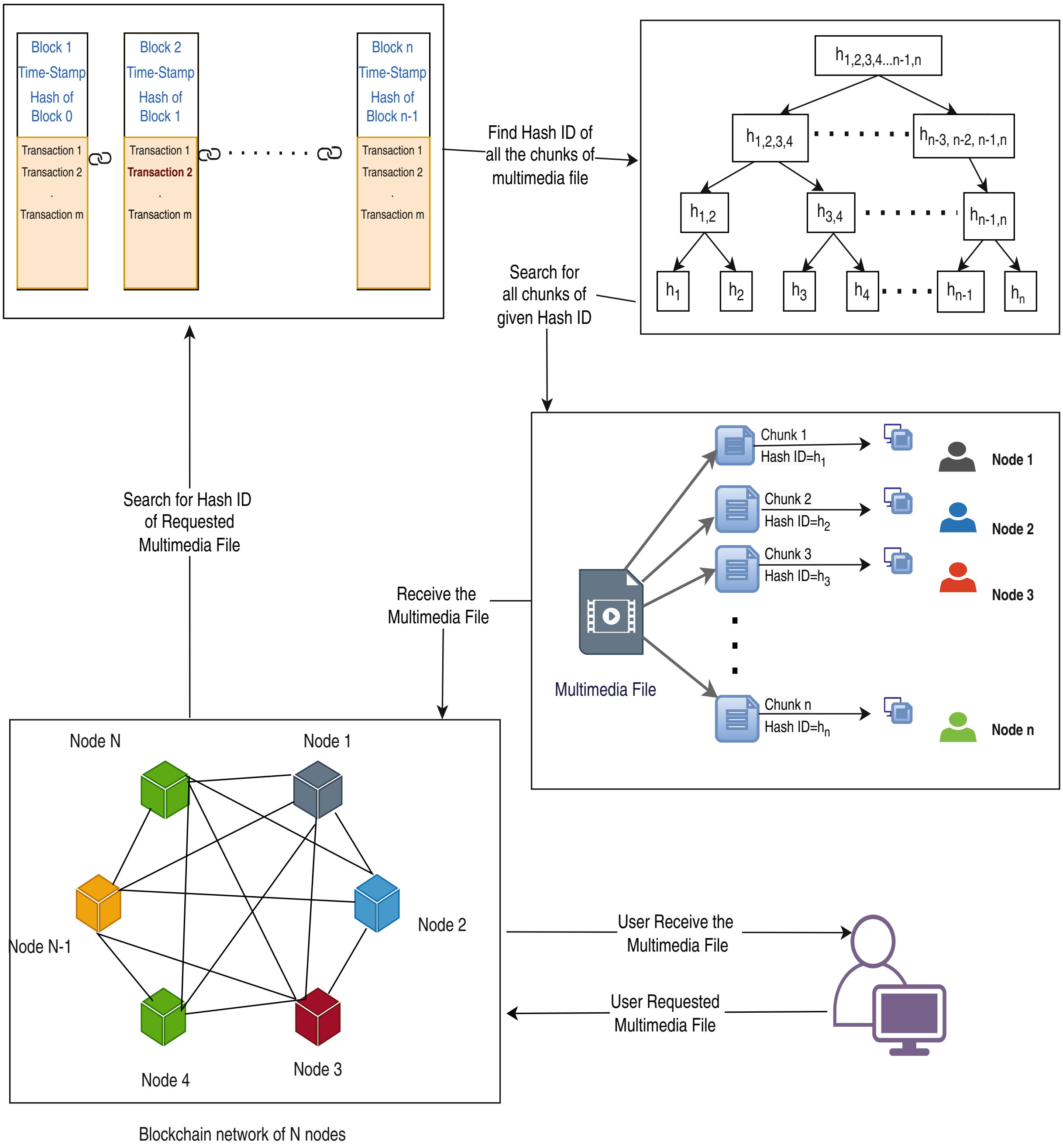


FIGURE 7 Working of system architecture

In our system framework, we have used the Schnorr user identity authentication protocol as shown in Figure 5. Note that we have used the non-interactive version of the authentication protocol to reduce the communication cost. After receiving the request from the user, the authentication process starts. If the user identity is successfully authenticated, then the multimedia file request moves forward to the next step by the blockchain network. Otherwise, the blockchain network rejects the request if the user cannot prove their identity to the network.

- *Step 2: Hash search*. After receiving the multimedia file request, the blockchain network process the proposal further. It will look for the hash id of the user's file asking for in their blockchain ledger. Since the blocks in the blockchain are linked to each other by using the hash id of the previous block, navigating for the specific hash id is easy. In Figure 7, blockchain is looking for the multimedia video file hash that is stored as transaction 2 in block 2 of the blockchain.

- *Step 3: File search*. In our system framework, each file is divided into several chunks, which is distributed among random peers or nodes of the network. After finding the unique hash id of the video file, the blockchain network looks for the hash id of all the chunks that all together will make the main file.

  For that, blockchain uses a generalization of the hash list called Merkle tree, a hash-based binary data structure. It is called the Merkle tree because of its tree-like structure in which each leaf node is a hash of a block of multimedia data file, and each non-leaf node is a hash of its children. Merkle trees have a branching factor of 2, meaning that each node has up to 2 children. Standard Merkle trees are implemented as binary trees; however, they can also be created as an *n*-nary tree, with *n* children per node. Figure 8 shows that an input file of multimedia data is broken up into blocks labeled *h*1 though *hn*. Each of these blocks is hashed using some hash function. Our system framework uses the bottom-to-top approach to get the original multimedia data file. So, each pair of nodes is recursively hashed until we reach the root node, a hash of all nodes below it. In our case, all these nodes define the hash of separate chunks of multimedia files.
- *Step 4: Response to user request*. After getting the hash id of all the chunks, it collects all the multimedia file chunks and recombines them into one original file. This multimedia file is then sent back to the user using the network.

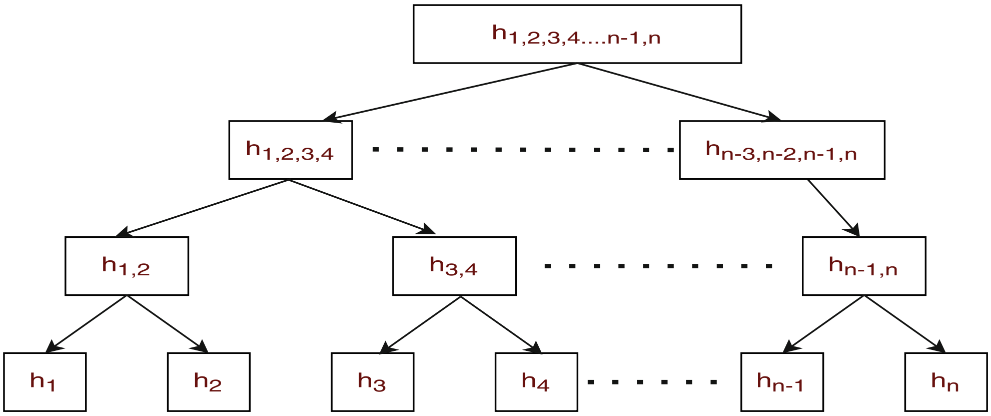


FIGURE 8 Merkle tree of hashes of multimedia data file

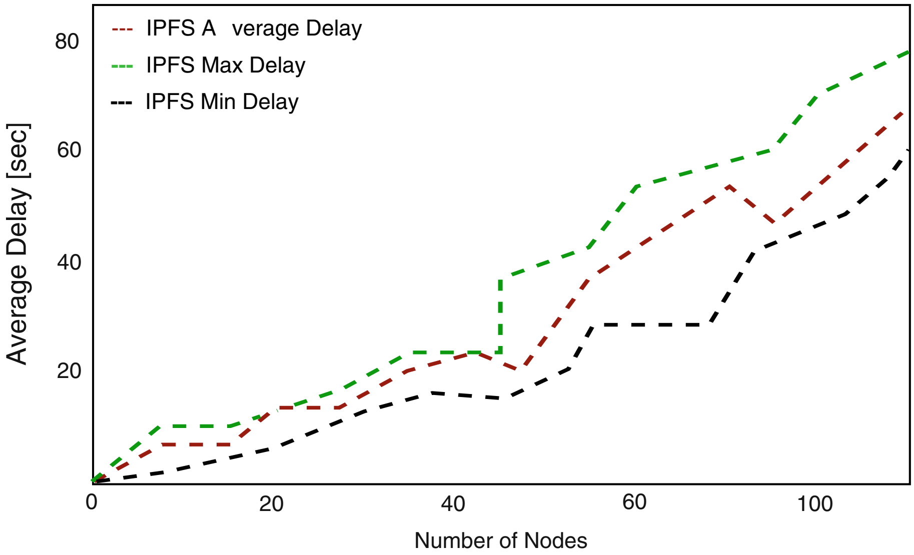


FIGURE 9 Average delay in IPFS depending on the number of nodes

TABLE 2 Security comparison of existing work with the proposed framework

Security against	Bhowmik and Feng[62]	Jan et al[63]	Our work
Leakage	✓	×	✓
Tampering	✓	✓	✓
Vandalism	×	✓	✓
Eavesdropping	×	✓	✓
Masquerading	×	×	✓
Message tampering	✓	✓	✓
Replaying	×	×	✓
Denial of service	✓	×	✓
Distributed denial of service	✓	×	✓

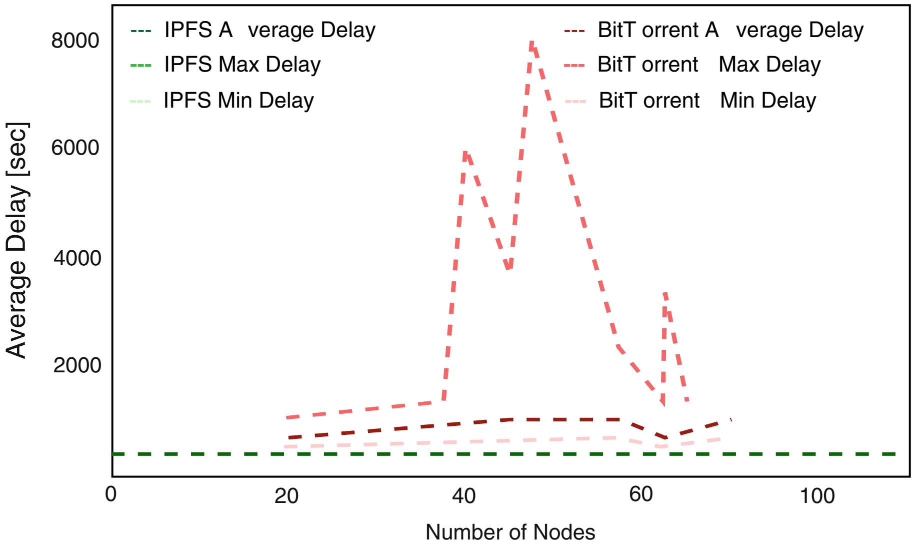


FIGURE 10 Comparison of IPFS performance with BitTorrent depending on the number of nodes

4.1 | Experimental results

Here we present the testing of our framework based on the IPFS performance using a script that is implemented based on the following steps:[61]

1. Add 10 MB file to IPFS daemon.
2. Create 1 to 100 IPFS daemons in different directories.
3. Do IPFS get from each daemon and measure the average time required to download the file.

Figure 9 shows the minimum delay, average delay and maximum delay in multimedia data file-sharing or exchanging in the IoT network that of course depends on the network crowd or number of nodes in the IoT network. Further, Figure 10 shows the comparison of minimum delay, average delay and maximum delay in IPFS as compared to other file-sharing systems such as BitTorrent. Comparison results are shown in Table 2.

5 | SECURITY ANALYSIS

Multimedia data may contain sensitive, confidential and private information. So, it is essential to discuss the associated risks and see to what level or extent our proposed system is secure. Therefore, this section will discuss the different types of security breaches and threats to the multimedia file system. We will also analyze the security of our system architecture against such attacks.

There are several risks associated with the distributed file-sharing system (see, eg, Reference 64) such as data leakage, data tampering, message tampering, replaying, and vandalism. Here data leakage includes eavesdropping attacks, data-tampering includes masquerading attacks, and vandalism includes denial of service attacks.

1. *Leakage*: Multimedia data leakage refers to the risk of having unauthorized nodes or users, also known as adversaries gaining access to sensitive or confidential information. We have introduced user or node authentication in our proposed system to prevent this type of data leakage. User authentication ensures that only authorized nodes or users access these multimedia data.
2. *Tampering*: Multimedia data tempering is another crucial security challenge as it has a solid potential to mislead the users or nodes by changing the information. Tampering multimedia data is the risk of having an adversary editing/altering or changing information that said user or node should not be able to edit or alter later. To prevent the tempering of data, we have used the blockchain system to store the hash of multimedia data files. If an adversary tries to temper the data, it will change the hash value of that file, and therefore, it will be easy to track the adversary by looking at the Merkle hash root.
3. *Vandalism*: Vandalism is when an adversary actively interferes with the operation of a system without any gain for themselves. As we already said, only authenticated users will have access to the system in our system architecture. It is significantly less likely that an adversary can launch a Vandalism attack.
4. *Eavesdropping*: An eavesdropping attack or sniffing attack refers to the theft of information when it is transmitted over a communication channel or network by a node or computer user, smartphone, or another device such as IoT-connected devices in our case. In this attack, the adversary targets the unsecured communication network to access multimedia data during the transfer phase between sender and receiver. We have used the IPFS system that utilizes the blockchain network to prevent this attack. As the blockchain network provides a high level of security, our system is safe from such attacks. It also ensures security against data leakage.
5. *Masquerading*: Masquerading refers to when an adversary tries to impersonate itself as another authenticated user, meaning that it tries to pretend another user's identity to communicate through the network. Since our authentication protocol is based on zero-knowledge proofs, which ensures a high level of user privacy and security, it is almost impossible for any adversary to masquerading.
6. *Message tampering*: Message tampering refers to an act when adversaries hack the message and tamper with the message during the message transmission phase between the communication network. For example, the sender sends a multimedia file to a receiver. An adversary intercepts this message, hacks the file, changes or tampers it, and then sends it to the receiver. A receiver may think that the delay in receiving the file is due to network congestion. So, the receiver gets the file but the malicious one.

   Man-in-the-middle attacks are one of the popular message tampering techniques. In this attack, the adversary intercepts the first key exchange. Then, it replaces the key with its key so that the adversary can decrypt messages being sent for the duration of that session. However, blockchain is secure against such attacks; therefore, our system automatically guarantees security against such attacks.
7. *Replaying*: Replaying is an act where an adversary saves and stores the intercepted message and keeps that message for later use. For example, an adversary can use the previously stored intercepted message to prove the identity or impersonate the authenticated user—this kind of attack work well even for authenticated and encrypted messages.

   Blockchain has an excellent property that if the transaction is saved with the time stamp and its hash value will be recorded forever in the ledger. So, if someone wants to use the intercepted message to do the same or other transaction, it will be easily caught by the system. Therefore, by using the blockchain ledger to store the hash value of the multimedia file, we make our system secure against such attacks.
8. *Denial of service*: Denial of service attacks is when an adversary starts to jam the communication network by sending several fake messages—doing so slows the communication network's speed and can take advantage of such network congestion. The attack is sometimes used to destroy or spoil the communication channel. However, this is not possible

in the IPFS system because the latency of the IPFS system is very high. Therefore, the adversary cannot have the opportunity to launch such an attack.

9. *Distributed denial of service*: Distributed denial of service attack has similarities to a regular denial of service attack. The main difference between these two attacks is the magnitude of the attack possible by an adversary. A distributed denial of service attack uses entire communication networks of compromised IoT devices to jam or flood the communication channels with much more traffic than is possible with a regular denial of service attack.

6 | CONCLUSION

Sharing a multimedia file such as audio-video or big text files among the wireless IoT network is not easy when one node cannot trust the other nodes completely. Also, keeping the file-sharing system centralized has another problem. Suppose if that server or mediator is malicious, it will completely spoil the whole data exchange network. We have proposed a decentralized system framework for sharing and exchanging the multimedia file system over a wireless IoT network to solve such a problem. We have used the blockchain and IPFS system to provide high security without compromising latency. Therefore, our proposed multimedia data file sharing system is very fast as it gives high latency and is highly secure. Our proposed framework is highly secure compared to the others as shown in Table 2. Integrating blockchain with IoT has either a throughput scalability issue or a security issue. However, to overcome this issue we have used the IPFS file-sharing system and stored only the hash of these files which improves the scalability and latency drastically. As a future direction, the research has strong potential to extend to build a secured distributed detection system based on IPFS and blockchain for industrial image and video data security. Also our proposed system can be further researched for IoT-based e-health applications by implementing a blockchain-based attack detection on machine learning algorithms.

ACKNOWLEDGMENT

The work of Shalini Dhar is supported by University Grant Commission (UGC) Fellowship for PhD students.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Rajani Singh https://orcid.org/0000-0002-9997-5830

REFERENCES

1. What is multimedia? 2021. https://www.geeksforgeeks.org/what-is-multimedia/
2. Multimedia introduction. https://www.tutorialspoint.com/multimedia/multimedia_introduction.htm
3. IoT, sensor, and cloud server. https://www.webnms.com/iot/help/iot_deployment_guide_cloudgate/iot,_sensors,_and_cloud_server.html
4. Types of communications in IOT; 2021. https://www.geeksforgeeks.org/types-of-communications-in-iot/
5. Communication models in IoT (Internet of Things); 2021. https://www.geeksforgeeks.org/communication-models-in-iot-internet-of-things/
6. Wireless network; 2016. https://www.techopedia.com/definition/26186/wireless-network
7. Wireless network; 2022. https://www.fortinet.com/resources/cyberglossary/wireless-network
8. What is wireless network. https://www.home-network-help.com/wireless-network.html
9. Wu JMT, Li Z, Srivastava G, Yun U, Lin JCW. Analytics of high average-utility patterns in the industrial Internet of Things. *Appl Intell*. 2022;52(6):6450-6463.
10. Khalid U, Asim M, Baker T, Hung PC, Tariq MA, Rafferty L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust Comput*. 2020;23(3):2067-2087.
11. Srivastava G, Lin JCW, Zhang X, Li Y. Large-scale high-utility sequential pattern analytics in Internet of Things. *IEEE Internet Things J*. 2021;8(16):12669-12678. doi:10.1109/JIOT.2020.3026826
12. Ahmed U, Lin JCW, Srivastava G. Unmanned aerial multi-object dynamic frame detection and skipping using deep learning on the internet of drones. *IEEE Internet Things Mag*. 2021;4(4):36-39. doi:10.1109/IOTM.001.2100088
13. Lin JCW, Srivastava G, Zhang Y, Djenouri Y, Aloqaily M. Privacy-preserving multiobjective sanitization model in 6G IoT environments. *IEEE Internet Things J*. 2021;8(7):5340-5349. doi:10.1109/JIOT.2020.3032896
14. Roy AK, Nath K, Srivastava G, Gadekallu TR, Lin JCW. Privacy preserving multi-party key exchange protocol for wireless mesh networks. *Sensors*. 2022;22(5):1958.

15. Dhall S, Dwivedi AD, Pal SK, Srivastava G. Blockchain-based framework for reducing fake or vicious news spread on social media/messaging platforms. *Trans Asian Low-Resource Lang Inf Process*. 2021;21(1):1-33.
16. Khullar K, Malhotra Y, Kumar A. Decentralized and secure communication architecture for FANETs using blockchain. *Proc Comput Sci*. 2020;173:158-170.
17. Majid M, Habib S, Javed AR, et al. Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: a systematic literature review. *Sensors*. 2022;22(6):2087. doi:10.3390/s22062087
18. Singh P, Singh N. Blockchain with IoT and AI: a review of agriculture and healthcare. *Int J Appl Evol Comput (IJAEC)*. 2020;11(4):13-27.
19. Kumar A, Saha R, Alazab M, Kumar G. A lightweight signcryption method for perception layer in Internet-of-Things. *J Inf Secur Appl*. 2020;55:102662. doi:10.1016/j.jisa.2020.102662
20. Khattak HA, Shah MA, Khan S, Ali I, Imran M. Perception layer security in Internet of Things. *Futur Gener Comput Syst*. 2019;100:144-164. doi:10.1016/j.future.2019.04.038
21. Dwivedi AD, Singh R, Ghosh U, Mukkamala RR, Tolba A, Said O. Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things. *J Ambient Intell Humaniz Comput*. 2021. 10.1007/s12652&hyphen;021&hyphen;03459&hyphen;4
22. Lucia O, Isong B, Gasela N, Abu-Mahfouz AM. Device authentication schemes in IoT: a review; 2019:1-6.
23. Wu H, Dwivedi AD, Srivastava G. Security and privacy of patient information in medical systems based on blockchain technology. *ACM Trans Multimed Comput Commun Appl*. 2021;17(2s):60. doi:10.1145/3408321
24. Singh R, Dwivedi AD, Srivastava G. Internet of Things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensors*. 2020;20(14):3951. doi:10.3390/s20143951
25. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. *Wirel Netw*. 2014;20(8):2481-2501. doi:10.3390/s20143951
26. Banotra A, Sharma JS, Gupta S, Gupta SK, Rashid M. Use of blockchain and Internet of Things for securing data in healthcare systems; 2021:255-267; Springer.
27. Peng SL, Pal S, Huang L. *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*. Switzerland: Springer; 2020.
28. Jain A, Singh T, Jain N. Framework for securing IoT ecosystem using blockchain: use cases suggesting theoretical architecture; 2021:223-232; Spinger.
29. Sodhro AH, Pirbhulal S, Muzammal M, Zongwei L. Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications. *J Grid Comput*. 2020;18(4):615-628.
30. Dwivedi AD, Srivastava G, Dhar S, Singh R. A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors*. 2019;19(2):326.
31. Sharma P, Jindal R, Borah MD. Healthify: a blockchain-based distributed application for health care. In: Suyel N, Ganesh CD, eds. *Applications of Blockchain in Healthcare*. Singapore: Springer; 2021:171-198.
32. Dwivedi AD, Singh R, Dhall S, Srivastava G, Pal SK. Tracing the source of fake news using a scalable blockchain distributed network. 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems; 2020:38-43; IEEE.
33. Biswas S, Sharif K, Li F, Latif Z, Kanhere SS, Mohanty SP. Interoperability and synchronization management of blockchain-based decentralized e-health systems. *IEEE Trans Eng Manag*. 2020;67(4):1363-1376.
34. Kaushik K, Dahiya S, Singh R, Dwivedi AD. Role of blockchain in forestalling pandemics; 2020:32-37; IEEE.
35. Alsamhi SH, Lee B, Guizani M, Kumar N, Qiao Y, Liu X. Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: framework and proposed solutions. *Trans Emerg Telecommun Technol*. 2021;32(9):e4255.
36. Alam T. mHealth communication framework using blockchain and IoT technologies. *Int J Sci Technol Res*. 2020;9(6):1-7.
37. Alsamhi SH, Lee B. Blockchain-empowered multi-robot collaboration to fight COVID-19 and future pandemics. *IEEE Access*. 2020;9:44173-44197.
38. Murugan A, Chechare T, Muruganantham B, Kumar SG. Healthcare information exchange using blockchain technology. *Int J Electr Comput Eng*. 2020;10(1):421.
39. Jennath H, Anoop V, Asharaf S. Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence. *Int J Int Multimed Artif Intell*. 2020;6.
40. Xu R, Chen Y, Blasch E. Decentralized access control for IoT based on blockchain and smart contract. In: Charles AK, Laurent LN, Alexander K, Sachin S, eds. *Model Des Secure IoT*. 2020:505-528.
41. Prabhu V. *Decentralized Decision Making for Limited Resource Allocation Using a Private Blockchain Network in An IoT (Internet of Things) Environment with Conflicting Agents*. PhD thesis. Clemson University, 2020.
42. Sharma A, Tomar R, Chilamkurti N, Kim BG. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics*. 2020;9(10):1609.
43. Gerrits L, Kromes R, Verdier F. A true decentralized implementation based on iot and blockchain: a vehicle accident use case; 2020:1-6; IEEE.
44. Hewa T, Braeken A, Ylianttila M, Liyanage M. Multi-access edge computing and blockchain-based secure telehealth system connected with 5G and IoT; 2020:1-6; IEEE.
45. Dwivedi AD, Morawiecki P, Singh R, Dhar S. Differential-linear and related key cryptanalysis of round-reduced scream. *Inf Process Lett*. 2018;136:5-8.
46. Dwivedi AD, Dhar S, Srivastava G, Singh R. Cryptanalysis of round-reduced fantomas, robin and iSCREAM. *Cryptography*. 2019;3(1):4.
47. Dwivedi AD. Security analysis of lightweight IoT Cipher: Chaskey. *Cryptography*. 2020;4(3):22. doi:10.3390/cryptography4030022

48. Yazdinejad A, Srivastava G, Parizi RM, Dehghantanha A, Choo KKR, Aledhari M. Decentralized authentication of distributed patients in hospital networks using blockchain. *IEEE J Biomed Health Inform*. 2020;24(8):2146-2156.
49. Aujla GS, Jindal A. A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. *IEEE J Select Areas Commun*. 2020;39(2):491-499.
50. Aboushosha B, Ramadan RA, Dwivedi AD, El-Sayed A, Dessouky MM. SLIM: a lightweight block cipher for internet of health things. *IEEE Access*. 2020;8:203747-203757.
51. Dwivedi AD. Brisk: dynamic encryption based cipher for long term security. *Sensors*. 2021;21(17):5744.
52. Gadekallu TR, Manoj M, Kumar N, et al. Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. *IEEE IoT Mag* 2021; 4(3): 30–33.
53. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. Blockchain leveraged decentralized IoT eHealth framework. *IoT*. 2020;9:100159.
54. Qu Y, Gao L, Luan TH, et al. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet Things J*. 2020;7(6):5171-5183.
55. Ray PP, Kumar N, Dash D. BLWN: blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare. *IEEE Syst J*. 2020;15(1):134-145.
56. Celesti A, Ruggeri A, Fazio M, Galletta A, Villari M, Romano A. Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. *Sensors*. 2020;20(9):2590.
57. MD5 Hash generator; 2022. https://www.md5hashgenerator.com/
58. IPFS: a decentralised cloud and file system for the blockchain environment; 2020. https://www.opensourceforu.com/2020/08/ipfs-a-decentralised-cloud-and-file-system-for-the-blockchain-environment/
59. Using IPFS for distributed file storage systems; 2020. https://medium.com/0xcode/using-ipfs-for-distributed-file-storage-systems-61226e07a6f
60. How to integrate IPFS with Ethereum; 2021. https://www.quicknode.com/guides/web3-sdks/how-to-integrate-ipfs-with-ethereum
61. IPFS performance. https://github.com/ipfs/go-ipfs/issues/5226.
62. Bhowmik D, Feng T. The multimedia blockchain: a distributed and tamper-proof media transaction framework; 2017:1-5; IEEE.
63. Jan MA, Cai J, Gao XC, et al. Security and blockchain convergence with Internet of Multimedia Things: current trends, research challenges and future directions. *J Netw Comput Appl*. 2021;175:102918.
64. Coulouris G, Dollimore J, Kindberg T, Blair G. *Distributed Systems: Concepts and Design. Computer*. Vol 4. 5th ed. Amsterdam: Elsevier; 2011.

How to cite this article: Dhar S, Khare A, Singh R. Advanced security model for multimedia data sharing in Internet of Things. *Trans Emerging Tel Tech*. 2022;e4621. doi: 10.1002/ett.4621