International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.7 March - April – 2023
DOI:10.46647/ijetms.2023.v07i02.071 ISSN: 2581-4621

A SURVEY ON EFFICIENT AUDITING SCHEME FOR SECURE DATA STORAGE IN FOG-TO-CLOUD COMPUTING

A.Thenmozhi[1], Dr.D.Vanathi M.E, PhD[2]
[1]PG Scholar, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India
[2]Head of the Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India

ABSTRACT

With the rise of the Internet of Things, fog-to-cloud computing has emerged as a new cutting-edge approach (IoT). Except for the cloud service provider, fog-to-cloud computing necessitates the participation of additional entities, such as mobile sinks and fog nodes (CSP). As a result, fog-to-cloud storage integrity audits will differ from standard cloud storage auditing. Tian et al. has completed the first stage in developing a public auditing system for fog-to-cloud computing. However, because they employ complex public key cryptography techniques like bilinear mapping and proof of knowledge, their system becomes inefficient. We offer a more broad and efficient auditing system based on MAC and HMAC, two prominent private key cryptography algorithms in this study. By implementing MAC and HMAC, we give a real instantiation of our auditing system. Finally, theoretical analysis and actual findings show that our suggested system has lower communication and computing costs.

Keywords: Media Access Control, Homomorphic MAC, Cloud Storage, Fog-to-cloud computing.

1. INTRODUCTION

Fog computing, initially presented by Bonomi et al. in 2012, has since become a popular approach for several industrial domains based on Internet-of-Things (IoT) devices. As a middleware between IoT devices and clouds, fog computing nodes have their own basic computing, storage, and resources to meet the needs for data pre-processing and transfer. As a result, the fog-to-cloud computing paradigm appears as a promising alternative for data storage in several resource-constrained large-scale industrial applications. However, fog-to-cloud computing must deal with some of the same issues that plague regular cloud computing. One of the most well-known problems is how to protect the integrity of data kept by a cloud service provider (CSP). The cause is as follows. Certain CSPs may attempt to disguise the fact that some critical data from IoT devices or fog nodes has been lost or damaged as a result of internal or external assaults. As a result, much as in traditional cloud computing, creating effective auditing tools for safe data storage in fog-to-cloud computing is critical. Although various auditing methods for traditional cloud storage have been published in recent years, including several private and public auditing schemes, all of them are not immediately relevant to fog-to-cloud computing for two key reasons.

1.1 MAC (Media Access Control)

A media access control address (MAC address) is a network-wide identification for an Ethernet or network adaptor. It identifies various network interfaces and is used for a variety of network technologies, most notably most IEEE 802 networks, including Ethernet. MAC addresses appear in the OSI model's Media Access Control Protocol sub-layer. The vendor/manufacturer of each network interface card (NIC) created normally assigns MAC addresses. They are used in almost all network types, however unlike IP addresses, MAC addresses are fixed and cannot be modified. IEEE guidelines are used to generate a MAC address. Each MAC address is a 12-digit hexadecimal notation stored inside the NIC firmware, consisting of a six-digit manufacturer's organisation unique identification followed by a six-digit serialised or random unique identity. Contention is based on a first-come, first-served basis. The most common contention-based MAC protocol used in Ethernet networks is carrier sense multiple access/collision detection (CSMA/CD). When a device needs to transmit, the NIC checks the network to see if another device is sending. If the NIC detects electrical signals on the network indicating that another device is broadcasting, it cannot communicate.

1.2 HOMOMORPHIC MAC

Network coding is an alternative routing strategy to traditional ‘store-and-forward' techniques. It enables intermediary nodes to change packets while they are in transit. It is commonly known that network coding may improve network speed and robustness. However, it is the trait of message mixing that renders network coding vulnerable to pollution attacks. Homographic message authentication codes (MACs) have been offered as a solution to this problem. To authenticate a message with a tag over a field, current Homomorphic MAC techniques use inner product. In practise, the size of the field is usually selected (or wanted) to be modest (often set to 28) in order to reduce computational and communication overheads. An opponent will crack the schemes with a probability of at least 1/q1/q (usually 1/281/28) in these circumstances. In this circumstance, security is not guaranteed. To overcome the limits and improve security, several tags are used for each message, which incurs significant key size cost and is not recommended in applications.

1.3 CLOUD STORAGE

Cloud storage is a cloud computing concept in which data is stored on the Internet by a cloud computing provider who maintains and administers data storage as a service. It is offered on demand with just-in-time capacity and rates, and it eliminates the need for you to purchase and manage your own data storage infrastructure. Cloud storage is simply a virtual vault where we may store any of our data remotely. When we upload a file to a cloud-based server, such as Google Drive, One Drive, or cloud, it is replicated via the Internet onto a data server, which is a physical location where businesses store files on several hard drives. Most businesses have hundreds of these servers, dubbed "server farms," spread over numerous sites. So, if our data is somehow lost, we will not lose it since it will be backed up somewhere else. This is known as redundancy, and it protects our data from loss. Despite being saved in the cloud, our data still need physical storage.

1.4 FOG -TO- CLOUD COMPUTING

Fog computing is a type of decentralised computing infrastructure in which data, compute, storage, and applications are distributed between the data source and the cloud. Fog computing, like edge computing, brings the benefits and capability of the cloud closer to where data is produced and acted on. Because both entail moving intelligence and processing closer to where the data is produced, many people use the words fog computing and edge computing interchangeably. This is frequently done to increase productivity, but it may also be done for security and compliance concerns. The fog metaphor is derived from the meteorological word meaning a cloud near the ground, exactly as fog concentrates on the network's edge. The name is frequently linked with Cisco; Ginny Nichols, the company's product line manager, is said to have created it. Cisco Fog Computing is a trademark; fog computing is available to the general public. Cloud computing is supplemented by fog networking, not replaced by it; fogging enables short-term analytics at the edge, while the cloud does resource-intensive, longer-term analytics. Although edge devices and sensors create and collect data, they often lack the computation and storage capabilities required to execute advanced analytics and machine learning activities. Though cloud servers have the capability to do so, they are frequently too far away to process the data and reply in a timely manner.

2. LITERATURE SURVEY

Charm: A Framework for Rapidly Prototyping Cryptosystems In this study, Joseph A et al.[1]presented Charm, an extensible framework for rapidly developing cryptographic systems. Charm has a number of features that expressly facilitate the construction of new protocols, such as support for the modular composition of cryptographic building blocks, infrastructure for designing interactive protocols, and a large library of reusable code. In addition, our framework includes a set of specialised tools that allow different cryptosystems to communicate with one another. We used Charm to construct over forty cryptographic algorithms, including several that had never been developed before. This article outlines our modular design, which includes a built-in benchmarking module for comparing the performance of Charm primitives to current C implementations.

Homomorphic MACs: MAC-based Integrity for Network CodingShweta Agawam et al. [2] suggested network coding in this research, which has been proved to increase network capacity and robustness. However, because intermediary nodes change packets en route, standard MACs and checksums cannot be used to verify data integrity. Furthermore, network coded systems are subject to pollution attacks, in which a single rogue node may flood the network with incorrect packets, preventing the receiver from correctly decoding the packets. To counteract such attacks, signature methods have been developed, however they are typically too slow for online per-packet integrity.

Provable Data Possession at Untrusted Stores.[3] We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant number of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees.

Proofs of Storage from Homomorphic Identification Protocols [4] GiuseppeAteniese and others Proofs of storage (PoS) are interactive protocols described by Al. in this study that allow a client to verify that a server faithfully stores a file. Previous research has demonstrated that storage proofs may be generated using any Homomorphic linear authenticator (HLA). In general, the latter are signature/message authentication techniques in which 'tags' from several messages may be homomorphically coupled to provide a 'tag' on any linear combination of these messages. We present a framework for constructing public-key HLAs from any identifying protocol that meets certain Homomorphic requirements. We next demonstrate how to convert any public-key HLA into a publicly-verifiable Po's with communication complexity independent of file length and an infinite number of verifications.

Dynamic Data Possession in Cloud Computing Systems In this research, Ayad F et al.[5] claim that an increasing number of enterprises are outsourcing data to remote cloud service providers (CSPs). Customers can hire the CSP's storage infrastructure to store and retrieve a nearly limitless amount of data for a monthly cost measured in gigabytes. Some clients may want their data duplicated on several servers across various data centres for enhanced scalability, availability, and durability. Customers are charged extra costs when the CSP is required to hold more copies. Clients must thus have a solid guarantee that the CSP is storing all data copies agreed upon in the service contract, and that all of these copies are compatible with the most recent updates given by the customers.

Fog computing with the integration of Internet of things: Architecture, Applications and Future DirectionsHeena Wadhwa [6] proposed in this study that the Information Technology business is competitive due to the technical environment. In this climate, the usage of cloud services has grown in order to provide high-quality services and quick product delivery to cloud consumers. However, several concerns remain unaddressed, particularly those relating to latency between the cloud data centre and the end user. With the collaboration of cloud computing, fog computing is employed to satisfy the rising demand for IT services. It offers cloud computing and storage services close to IoT devices. The term "fog computing" refers to the advancement of cloud-based network and computer services. This article addresses the concept, architecture, and application of fog computing.

Proofs of Irretrievability: Theory and Implementation [7] A proof of retrievability (POR) is a compact evidence by a file system (prover) to a client (verifier) that a target file F is intact, in the sense that the client can completely recover it, as proposed by Kevin D et al. in this work. PORs are an appealing building component for high-assurance remote storage systems because they have lesser communication complexity than F transmission. We present a theoretical framework for the design of PORs in this study. We show that effective encoding is possible even for files F that are larger than the client's main memory. Cloud computing, or the loosely connected networking of computational resources, is detaching data from local storage platforms. Users today frequently access files without knowing what computers or geographical regions their files are stored on.

Secure network coding from secure proof of retrievability [8] .In this paper, Jinyong CHANG et al. propose that network coding is a more appealing paradigm than traditional storing-and-forwarding routing mechanisms because it has been demonstrated capable of achieving maximum throughput, enhanced robustness, and lower energy consumption for communication networks. Unfortunately, this paradigm is extremely vulnerable to contamination. More particular, if a packet is unlawfully modified (i.e., a polluted packet), the modification may swiftly propagate throughout the network since the intermediary node encodes all received packets, including the polluted one. As a result, it is necessary for intermediate and terminal nodes to determine whether a data packet has been polluted, which is also the goal of the secure network coding (NC) technique.

RKA Security for Identity-Based Signature Scheme [9] In this research, JINYONG CHANG et al. introduced T Related-key attack (RKA) is a type of side-channel attack studied for many cryptographic primitives such as public key encryption, digital signature, pseudorandom functions, and so on. However, we notice that RKA-security does not appear to be taken into account for identity-based signature (IBS), an important basic for identity-based cryptography suggested by Shamir in 1984. In this research, we incorporate RKA security into IBS schemes for the first time and attempt to describe the security model for it. More precisely, we investigate the RKA that happens in the users' signature key or the master key of the key-generation centre (KGC), from which two types of RKA securities for IBS are derived. Meanwhile, by launching a basic RKA, we show that the most efficient Schnorr-like IBS method suggested by Galindo and Garcia is RKA-insecure.

Proofs of Retrievability via Hardness Amplification [10]Proofs of Retrievability (PoR), presented by Juels and Kaliski, allow the client to store a file F on an untrusted server and afterwards execute an efficient audit protocol in which the server shows that it (still) owns the client's data, as described by Yevgeniy Dodis et al. in this study. PoR scheme designs seek to reduce client and server storage, audit communication complexity, and even the amount of file-blocks viewed by the server during the audit. We identify many different issue variations (such as bounded-use vs. unbounded-use, knowledge-soundness vs. information-soundness) and provide nearly optimum PoR strategies for each of these variants in this work. Our constructs either improve (or expand) previous PoR constructions or provide the first known PoR schemes with the necessary features.

Blockchain-based Dynamic Provable Data Possession for Smart Cities [11] In this research, Ruonan Chen et al. claim that smart cities are rapidly developing due to developments in information and communication technologies such as the Internet of Things (IoT). To address the data storage concerns created by large-scale data generated by IoT devices, a growing number of businesses and people are opting to outsource their data to the cloud, where data integrity has become a worry for cloud users. So far, a number of proven data possession (PDP) methods for centralised cloud storage situations have been presented. However, centralised cloud depends too heavily on the trust of central servers and is thus vulnerable to single point of failure. We define a block chain-based PDP model to realise a decentralised outsourced storage framework in this research, and then demonstrate a realistic design of decentralised proven data possession utilising multi-replica storage techniques.

PORs: Proofs of Retrievability for Large Files [12] In this study, we define and investigate retrievability proofs presented by Ari Juels et al (PORs). A POR technique allows an archive or backup service (prover) to provide succinct proof that a user (verifier) can retrieve a target file F, i.e. that the archive maintains and reliably sends file data sufficient for the user to recover F in its entirety. A POR is similar to a cryptographic proof of knowledge (POK), but it is specifically built to handle huge files (or bitstrings) F. In this section, we look some POR protocols in which the communication costs, number of memory accesses for the prover, and storage needs of the user (verifier) are all tiny factors that are essentially independent of F length.

Compact Proofs of Retrievability [13] under this study, HovavShacham et al. suggest that in a proof-of-retrievability system, a data storage centre must demonstrate to a verifier that he is truly keeping all of a client's data. In this study, we present the first proof-of-retrievability algorithms in the strongest model, that of Juels and Kaliski, with comprehensive demonstrations of security against arbitrary attackers. Our first technique, based from BLS signatures and safe in the random oracle model, has the quickest query and response time of any public-verifiable proof-of-retrievability scheme. Our second technique, which is secure in the standard model and is built elegantly on pseudorandom functions (PRFs), has the quickest reaction time of any proof-of-retrievability scheme with private verifiability (but a longer query).

An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data [14] with the fast growth of cloud computing, cloud storage has been adopted by a growing number of enterprises and individuals, acting as a handy and on-demand outsourced application, as presented by Jian Shen et al. in this study. However, once users lose local control of their data, it becomes critical for them to check whether cloud service providers have safely kept their data. As a result, numerous academics have dedicated themselves to developing auditing techniques for outsourced data. In this research, we offer an efficient public auditing protocol with global and sampling block less verification, as well as batch auditing, where data dynamics are supported far more effectively than the state of the art.

Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage [15] In this research, Hui Tian et al. argue that Cloud storage is an increasingly popular use of cloud computing that may provide on-demand outsourced data services for both enterprises and individuals. However, consumers may not completely trust cloud service providers (CSPs) since it is difficult to ascertain whether the CSPs satisfy their legal data security obligations. As a result, it is vital to establish effective auditing tools in order to increase data owners' trust and confidence in cloud storage. We introduce a unique public auditing technique for safe cloud storage based on dynamic hash table (DHT), a new two-dimensional data structure situated at a third parity auditor (TPA) to store data property information for dynamic auditing, in this work.

Providing Data Dynamics and Public Accountability [16] Storage Security in Cloud Computing Qian Wang et al. propose cloud computing as the next-generation architecture of IT firms in this study. It moves the application. Software and databases to massively centralised data centres where data and service administration may not be fully automated trustworthy. This unique paradigm raises various new security concerns that are currently unknown. This undertaken analyses the subject of ensuring data storage integrity in cloud computing. In specifically, we discuss the task of allowing a third party. A third-party auditor (TPA) certifies the integrity of the dynamic data stored in the cloud on behalf of the cloud customer.

Public Auditing with Privacy Protection for Protected Cloud Storage [17] Cong Wang et al. argued in this study that customers can remotely store their data and experience on-demand high-quality apps and services by using cloud storage. without the expense of local data storage and upkeep, from a shared pool of flexible computer resources However, the reality is Because users no longer have physical custody of the outsourced data, data integrity protection in cloud computing is a concern. A difficult process, especially for consumers with limited computational resources Furthermore, consumers should be able to simply use the cloud. Storage as though it was local, without the need to validate its integrity. As a result, offering public audit ability for cloud storage is critical.

Remote Data Integrity Checking Using Identity Ideal Data Privacy Protection for Cloud Storage [18] In this research, Yong Yu et al. suggest that remote data integrity checking (RDIC) provides a to demonstrate to a data storage server, such as a cloud server validator that it is honestly storing a data owner's data A variety of RDIC protocols have been proposed in the past. The literature, yet nearly all of the structures suffer from They rely on the issue of complicated key management. costly public key infrastructure (PKI), which may impede RDIC implementation in practise. We suggest in this paper a new identity-based (ID-based) RDIC protocol construction by employing key-Homomorphic cryptography primitives to decrease system complexity and establishment costs as well as administering the PKI public key authentication framework Systems based on RDIC.

Auditing for Public Integrity in Dynamic Data Multi-User Modification Sharing [19] Jiawei Yuan the fast growth of cloud storage services in recent years has made it easier than ever for cloud users to exchange data with others. One another A variety of solutions have been proposed to ensure users' confidence in the integrity of their shared data in the cloud. For data integrity auditing with an emphasis on numerous practical aspects such as dynamic data support, public integrity auditing, and cheap cost Low storage overhead, low communication/computational audit cost However, most of these strategies assume that just the original data is relevant.

Cloud storage that is shown to be safe for mobile networks [20] fewer computations and lower overhead In this research, Rui ZHANG et al. offer Secure cloud storage (SCS), which ensures that data sent to the cloud remains intact. prior to outsourcing Previous techniques to ensuring cloud storage stability are either computationally intensive or inefficient. or permitting high overheads, and so are unsuitable for mobile networks with stringent computation/bandwidth constraints. Restrictions. We present an effective SCS system for mobile networks based on Homomorphic MAC in this study. And suggest domain expansion to increase the system's security and flexibility.

Kerberos Protocol with Improved Key Agreement for M-Health Security [21] in this research, P. Thirumoorthy et al. proposes the creation of a wireless sensor network using Internet of Things. (IoT) forecasts a variety of uses in healthcare and cloud computing. This has the potential to yield good outcomes in mobile health care (M-health) and Telerate. Information systems for medicine Internet of Things-based m-health system (IoT) via wireless sensor network (WSN) are a growing study area. the need of contemporary civilization Sensors placed to the patients' bodies that Being linked to a mobile device can make medical services more convenient. The first concern is security. crucial link for efficient operation of the m-health system that shares data of patients in wireless networks in order to protect their privacy .

Improved Energy-Use Multi-Sensor Object Detection in Wireless Sensor Networks Daniyal [22] Alghazzawi et al. suggest that independent sensor networks capable of sensing physical parameters like temperature, pressure, and humidity are distributed geographically within Wireless Sensor Networks (WSNs). Examples include energy, pressure, and sound. WSNs are resilient and have a secure connection to the physical environment. Data aggregation (DA) is an important part of WSN. helps cut down on energy use (EC). Existing research efforts have discovered DA with a high aggregation rate for WSNs in order to have reliable data. centred on DRINA (In-Network Aggregation Data Routing). Nevertheless, there is none. achieving an effective balance between routing and overhead; however, the EC DA requirements remained unmet.

Task scheduling in the cloud based on two stages Dynamic algorithm strategy [23] M.Deepika et al. presented in this study to improve task allocating performance and reduce illogical task allocation. Allocations in a cloud environment, this research proposes a two-stage technique. Strategy. Initially, a job classifier is driven by the design of a Naive Bayes classifier. The approach is used to classify occupations based on past scheduling data. Certain A number of virtual machines (VMs) of different sorts are built in response. This saves time. the time it takes to generate virtual machines during task allocation Jobs will be available in the next step.

An Investigation of a Routing Approach for In-Network Aggregation in Wireless Sensor Networks [24] In this paper, S.SUDHA et al. propose that we may construct data aggregation utilising the Data aggregation and routing techniques can help to lower the cost of Wireless sensor network communication Traffic congestion occurs when one or more of the many sensor nodes detects events. The network should inform the occurrence to save electricity. Only when an event occurs appropriately. Overhead happens in Because of its poor scalability, InFRA. According to the projected The DRINA algorithm (Data Routing for In-Network Aggregation) decreases communication costs and conserves energy.

Polynomial Distribution of Bayes Node Energy to Improve Wireless Sensor Routing Network [25] In this paper, Karthikeyan et al. propose a Wireless Sensor Network to monitor and manage the physical environment using a huge number of tiny sensors. low-cost sensor nodes Existing Wireless Sensor Network (WSN) technique given increased latency due to sensed data transfer via continuous data gathering as well as energy consumption To solve the routing problem and decrease energy consumption, The Bayes Node Energy and Polynomial Distribution (BNEPD) approach is presented. In a wireless sensor network, energy-aware routing is used.

3. COMPARATIVE ANALYSIS

Title	Techniques & Mechanisms	Parameter Analysis	Future Work
Charm: A Framework for Rapidly Prototyping Cryptosystems	We describe Charm, an extensible framework for rapidly prototyping cryptographic systems.	Compare the performance of Charm primitives to existing C implementations.	we plan to examine the possibility of compiling Charm code directly to languages such as Haskell and C, using tools such as Shedskin.
Homomorphic MACs: MAC-based Integrity for Network Coding	Homomorphic MAC. homomorphic MAC is defined by three probabilistic, polynomial-time algorithms	A homomorphic MAC which allows checking the integrity of network coded data.	whether a TESLA-type mechanism applied to our homomorphic MAC can be used to give the same functionality as our broadcast MAC.
Provable Data Possession at Entrusted Stores	We present two provably-secure PDP schemes that are more efficient than previous solutions. And RSA	As a basis of comparison, we have implemented the following two PDP schemes in addition to our E-PDP scheme:	Schemes also impose a significant I/O and computational 18 burden on the server and it had to be improved.
Proofs of Storage from Homomorphic Identification Protocols	We provide a framework for building public-key HLAs from any identification protocol satisfying certain homomorphic properties.	Combining our results, we obtain a publicly-verifiable proof of storage based on the factoring assumption in the random oracle model.	to obtain better performance while retaining public verifiability.
Provable Multi copy Dynamic Data Possession in Cloud Computing Systems	Map-based provable multi-copy dynamic data possession (MB-PMDDP) scheme.	We give a comparative analysis of the proposed MB-PMDDP scheme with a reference model obtained by extending dynamic single-copy schemes	the proposed scheme is based on using a small data structure (metadata), which we call a map-version table, which had be to improve in the future
Fog computing with the integration of Internet of things: Architecture, Applications and Future Directions	Fog computing is used to support increasing demand of IT service with the collaboration of cloud computing. It provides computational and storage services of cloud proximate to IoT devices.	it also compares different scheduling techniques on the basis of resource utilization, cost, network usage and latency that will provide an opportunity for all nascent researchers	The various issues that is generally faced in traditional cloud computing like network failure and high latency rate need to be improved.

Proofs of Retrievability: Theory and Implementation	The theoretical design of POR protocols that incorporates existing POR constructions, and enables design of new protocols with a wide range of parameter tradeoffs. we provided a Java implementation of the encoding algorithm of the new variant, in which files are processed and encoded incrementally.	We propose a new variant on the Juels-Kaliski protocol and describe a prototype implementation. We demonstrate practical encoding even for files F whose size exceeds that of client main memory.	An interesting practical problem is to design different encoding techniques with a minimal number of disk accesses for very large files, i.e., those for which the parity blocks do not fit into main memory.
Secure network coding from secure proof of retrievability	They proposed a general transformation from any secure NC scheme to secure PoR protocol. This connection immediately implies many previous secure NC schemes can automatically be used to construct secure PoR protocols.	The two properties of “Proof with linear-combination-form” and “Proof aggregation” guarantee that the intermediate nodes can correctly generate the combined packets in Combine.	Proof of retrievability (PoR) protocol is just one of initial attempts to formulize the notion of “remotely and reliably checking data’s integrity without downloading the whole data file. In future the reliability and remote access of data should be Improved.
RKA Security for Identity-Based Signature Scheme	We introduce the RKA security into IBS schemes and try to define the security model for it. More specifically, we consider the RKA occurs in the users’ signing key-generation center (KGC), which derives two kinds of RKA securities for IBS.	After slight modifying it, we can easily obtain RKA secure IBS scheme. Finally, we analyze the performance of the modified GG-scheme. We analyze the performance of the modified GG-scheme.	The performance of the modified GG scheme had to be improved in the future
Proofs of Retrievability via Hardness Amplification	Proofs of Retrievability (PoR) and PoR codes.	We make two observations about the prior work. Firstly, although all constructions implicitly use some form of PoR codes, such codes have not been defined.	To improve the efficiency of all known constructions. In particular, we show how to construct a variant of the computational scheme.

Block chain-based Dynamic Provable Data Possession for Smart Cities	we describe a block chain-based PDP model to realize decentralized outsourcing storage framework, and then present a concrete construction of decentralized provable data possession by using multi-replica storage tricks	We make use of multi-replica storage technique to enhance reliability and utilize block chain to record all transactions among peers. We prove its security in the random oracle model and implement the file storage algorithms of our protocol.	The future work is to investigate decentralized outsourced storage protocols with reward and punishment mechanisms
PORs: Proofs of Retrievability for Large Files	We introduce a sentinel-based POR scheme with several interesting properties: Of theoretical significance, the data in sentinels, and thus the resulting PORs, can be made independent of the stored file;	As storage-as-a-service spreads and users rely on external agents to store critical information, the privacy and integrity guarantees of conventional cryptography will benefit from extension into POR-based assurances around data availability.	Our introduction of PORs in this paper leads to a number of possible directions for future research.
Compact Proofs of Retrievability	BLS signatures and secure in the random oracle model and Pseudorandom functions (PRFs)	Both schemes rely on homomorphic properties to aggregate a proof into one small authenticator value.	A security proof against arbitrary adversaries need to be improved in the future
An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data	A public auditing protocol with a novel dynamic structure composed of a doubly linked info table and a location array.	Compared with the state of the art, an appropriate relationship between the DLIT and the LA makes our protocol perform better both in terms of efficient dynamic support and reduced overhead.	To Enhance the performance of the protocol in the future.
Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage	we present a novel public auditing scheme for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure located at a third parity auditor (TPA) to record the data property information for dynamic auditing.	Our scheme migrates the auditing metadata excerpt the block tags from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead.	It may be a new trend to design a more effective scheme, including different audit strategies for various types of cloud data in the future

Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing	The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing.	we explored the problem of providing simultaneous public audit ability and data dynamics for remote data integrity check in Cloud Computing	To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting,
Privacy-Preserving Public Auditing for Secure Cloud Storage	We propose a privacy-preserving public auditing system for data storage security in cloud computing.	We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server.	The full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large-scale data.
Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage	We propose a new construction of identity-based (ID-based) RDIC protocol by making use of key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI based RDIC schemes.	Secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier. Extensive security analysis and implementation results demonstrate that the proposed new protocol is provably secure and practical in the real-world applications	The security model need to be improved in the future.
Public Integrity Auditing for Dynamic Data Sharing with Multi-User Modification	The salient properties of public integrity auditing and constant computational cost on the user side.	innovative design on polynomial-based authentication tags which allows aggregation of tags of different data blocks.	To increase the efficiency of the r cloud data sharing services characterized by multi-user modification and high error detection probability in the future
Provably secure cloud storage for mobile networks with less computation and smaller overhead	Secure cloud storage (SCS) and homomorphic MAC	we implemented the proposed SCS system on a mobile device and a laptop respectively, and compared it with other schemes in theory and practice	To investigate enhanced SCS schemes with more functionality, such as dynamic data update or efficient public

			verifiability in the future.
Dynamic Audit Services for Outsourced Storages in Clouds	probabilistic query and periodic verification for improving the performance of audit services.	The performance of each activity in our verification protocol. It is easy to derive theoretically that the overheads of “commitment” and “challenge” resemble one another, and the overheads of“response” and “verification” also resemble one another	To minimize the computation and communication costs in the future by using various techniques.

4. CONCLUSION

We offer an effective auditing method for fog-to-cloud computing in this work. Although our system does not do public auditing, it clearly surpasses Tian et alin .'s terms of communication and computing efficiency. The results of the simulation demonstrate the computational efficiency. We feel that our suggested method is a compelling option for securely storing data in fog-to-cloud computing. In this paper, we describe and solve the issue of multi-keyword ranked search via encrypted Edge-Fog-Cloud data for the first time, as well as develop a variety of privacy constraints. We select the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, among various multi-keyword semantics to effectively capture the relevance of outsourced documents to the query keywords, and use "inner keyword similarity" to quantitatively evaluate such similarity measure.

5. REFERENCES

[1] J. C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. Akinyele "Charm: A Framework for Rapidly Prototyping Cryptosystems," D. Rubin, J. Cryptogr. English, vol. 3, no. 2, June 2013, pp. 111-128.
[2] S. D. Agrawal and Agrawal Applied Cryptography and Network Security (Lecture Notes in Computer Science), vol. 5536. Springer, Berlin, Germany, pp. 292-305, 2009.
[3] G. R. Burns, R. Curtmola, Joseph Herring, L. Kissner, Z. Peterson, and D. Ateniese "Provable data possession at untrustworthy retailers," Song, Proc. The 14th ACM Conf. Comput. Commun. 598-609, Secur., Alexandria, VA, USA, 2007.
[4] G. S. Kamara, Ateniese, and J. "Proofs of storage from homomorphic identification procedures," by Katz, published in Advances in Cryptology. Springer, Berlin, Germany, pp. 319-333, 2009.
[5] A. M. Barsoum and F. Barsoum "Provable multicopy dynamic data ownership in cloud computing systems," A. Hasan, IEEE Trans. Inf. Security Forensics, vol. 10, no. 3, March 2015, pp. 485-497
[6] F. R. Milito, J. Zhu, and S. Bonomi "Fog computing and its significance in the Internet of Things," Addepalli, Proc. 1st Ed. MCC Workshop Mobile Cloud Computing, New York, NY, USA, pp. 13-16, 2012.
[7] K. A. Juels, Bowers, and A. "Proofs of retrievability: Theory and application," Oprea, Proc. Cloud Computing ACM Workshop Secur., pp. 43-54, 2009.
[8] J. "Secure network coding from secure evidence of retrievability," Chang et al., Sci. Inf. China Science, early access, October 2020.
[9] J. H. Wang, F. Wang, A. Zhang, and Y. Chang IEEE Access, vol. 8, pp. 17833–17841, 2020.

[10] Y. S. Vadhan and D. Dodis "Proofs of retrievability by hardness amplification," by Wichs, in Proc. Cryptography Theory Conf., pp. 109-127, 2009.
[11] C. A. Küpçü, C. Papamanthou, and R. Erway "Dynamic proven data possession," Tamassia, Proc. CCS, 2009, pp. 213-222
[12] A. B. and Juels "PORs: Proofs of retrievability for huge files," J. Kaliski, Proc. The 14th ACM Conf. Comput. Commun. Secur., Alexandria, VA, USA, pp. 584-597, 2007.
[13] H. B. and Shacham "Compact proofs of retrievability," Waters, J. Cryptography, vol. 26, no. 3, pp. 442–483, 2013.
[14] J. J. Shen, X. Chen, X. Huang, and W. Shen Susilo, "An efficient public auditing technique for cloud data with a new dynamic structure," IEEE Trans. Inf. Security Forensics, vol. Oct. 2017, vol. 12, no. 10, pp. 2402-2415.
[15] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Zhu are the authors of the paper. "Dynamic-hash-table-based public auditing for secure cloud storage," by Liu, IEEE Trans. Serv. Computer Science, vol. 10, no. 5, September 2017, pp. 701-714.
[16] Q. C. Wang, K. Ren, W. Lou, and J. Wang "Enabling Public Auditability," Li and data dynamics for cloud storage security," IEEE Trans. Distrib. in parallel Vol. of Syst. May 2011, vol. 22, no. 5, pp. 847-859.
[17] Y. Z. L. Jiang, X. Wang, S. Yiu, and P. Wu "Dynamic data," Zhang activities with deduplication in public auditing for privacy protection safe cloud storage," according to Proc. IEEE International Conf. Comput. Sci. Eng. (CSE) IEEE International Conf. Ubiquitous Computing Embedded (EUC), July 17, 2017
pp. 21–24
[18] Y. G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Yu Min, "Identity-based remote data integrity verification with complete data privacy" IEEE Trans. on preservation for cloud storage," Inf. Security Forensics, vol. 12, no. 4, April 2017, pp. 767-778
[19] J. S. and Yuan "Public integrity auditing for dynamic data sharing with Yu," IEEE Trans. on Multiuser Modification," Inf. Security Forensics, vol. 10, no. 8, pages. 1717-1726, Aug. 2015
[20] R. H. Ma, Y. Lu, and Y. Zhang "Provably safe cloud storage for" Li "Mobile networks with lower computation and overhead," Sci. China Inf. Science, vol. 60, no. 12, 2017, p. 122104
[21] ThirumoorthyPalanisamy, D. Alghazzawi, S. Bhatia, A. A. Malibari, P. Dadheeche and colleagues, "Improved energy-based multi-sensor object recognition in wireless sensor networks," Intelligent Automation & Soft Computing, vol. 33, no.1, pp. 227–244, 2022.
[22] P. "Improved key agreement based kerberos protocol for m-health security," Thirumoorthy, K. S. Bhuvaneshwari, C. Kamalanathan, P. Sunita, E. Prabhu et al., Computer Systems Science and Engineering, vol. 42, no.2, pp. 577–587, 2022.
[23] M.Deepika, S.Prabhu, M.Parvathi, and S.Hemalatha, "Cloud Task Scheduling Using Dynamic Algorithm", Gradiva Review Journal, Vol.8, No. 11, pages 53-60, 2022.
[24] S. "A research on routing strategy for in-network aggregation in wireless sensor networks," Sudha, B. Manimegalai, and P. Thirumoorthy, in Proc, IEEE ICCCI, Coimbatore, India, pp.1-4, 2014.
[25] P. N. Thirumoorthy and Thirumoorthy "Bayes node energy polynomial distribution to optimise routing in wireless sensor networks," K. Karthikeyan, PLoS ONE, vol. 10, no. 10: e0138932, pp.1-15, 2015.