A Novel integrity and encryption based block-chain framework for e-governance cloud data

[1]Veera Raghava Rao Atukuri & [2]Ramineni Siva Rama Prasad

[1]Research Scholar, Department of Computer science and Engineering

[2]Professor & Head, Business Administration

[1,2]Acharya Nagarjuna University , Nagarjuna Nagar, Guntur, Andhra Pradesh.

Abstract

As the size of the media files are increasing in the public and private cloud servers, it is difficult to provide the data security due to file format and high dimensionality. Block-chain technology plays a vital role for large cloud databases. Most of the conventional block-chain frameworks are based on the existing integrity and confidentiality models. Also, these models are based on the data size and file format. In order to overcome these problems in the cloud computing environment, a hybrid integrity and security-based block-chain framework is designed and implemented on the large media data types. In this framework, a novel non-linear chaotic function-based hash algorithm and advanced attribute-based encryption models are used to improve the traditional block chain framework on the large cloud datasets. Experimental results proved that the proposed advanced block-chain technology has better efficiency than the traditional block-chain frameworks on the large cloud media files.

Keywords: Block-chain, Cloud computing, hash algorithm, encryption algorithm.

1.Introduction

Cloud computation is a most frequently used cloud service for both clients and organizations. It is responsible for processing data through virtual machines. It doesn't depend on the hardware and software specifications of clients' system. The virtual machines are not only simple to configure but also easy to integrate with different cloud storage. It can also be merged with other tools (for example Hadoop) for additional computation. Some commonly used cloud computation systems are: - Google Compute Engine, Windows azure, Amazon EC2 and Rackspace. Cloud computing offers an economical solution for the scalable and flexible success of the IT infrastructure. Cloud computing makes it easy for cloud users to provide the software and services, the deployment environment, storage space and computer resources on demand using a pay-by-use model. Cloud services can easily be provided by cloud providers and released by cloud users with minimum effort. Cloud providers transfer cloud user applications, software and databases to large data centers around the world and users cannot control the remote data directly. This unique feature of the cloud brings numerous new security challenges[1].

Cloud computing provides different types of cloud services for both clients and organizations. It is responsible for processing data through virtual machines. It doesn't depend on the software and hardware specifications of clients' system. The virtual machines are not only simple to configure but also easy to integrate with different cloud storage. It can

also be merged with other tools (for example Hadoop) for additional computation. Some commonly used cloud computation systems are: - Google Compute Engine, Windows azure, Amazon EC2 and Rackspace[2]. Public cloud: A Public cloud represents traditional cloud computing in which resources are continuously controlled over the Internet on a self-service basis. This is done by implementing a third party service provider which provides and shares bills and resources via a registered utility basis. This cloud service relies on a pay-per-use model similar to the power and energy metering scheme, making it very versatile and adaptable, thus attracting greater demand to leverage low security levels compared to other cloud models[3]. Cloud computing provides dynamically distributed services, as a service over the Internet. Third-party, on-demand, self-service, pay-per-use, and easily distributed computing resources and services provided through the cloud model are aimed at reducing the cost of hardware and software capital and operating costs. Clouds may be classified from the user's point of view to monitor the physical place. Third-party service providers offer a public cloud which requires resources outside the premises of the user. In the case that the cloud network is mounted at the user's house, in the data center itself, this configuration is generally called private cloud.

Confidentiality is a set of rules or a promise that restricts access or restricts certain types of information and ensures that the data is not disclosed to unauthorized persons. Proper steps should be taken to ensure sensitive information does not reach unauthorized persons, while ensuring that it is actually obtainable by the authorized persons. Some popular mechanisms for privacy assurance include encryption, passwords, biometric verification, smart card, computer tokens and so on. Cryptographic encryption is preferred as the appropriate means of confidentiality of the data. Privacy is paramount in the cloud environment. An identity theft has a greater impact on a cloud-based enterprise than on the premises. Cloud offers inherent benefits but businesses need to make decisions based on cost associations. Cloud computing is important for storing data and for accessing data in remote areas. The most important challenge in cloud computing because of this data storage is secure messaging. The user has no control over the data which is stored on remote servers. Hence the most difficult task in cloud computing is to secure data files from the cloud. Since, all data must be stored in a data storage platform, without authenticity. That leads to unsafe communication if any of the third parties can access the data. The data leakage is highly possible in cloud storage systems[4].The main benefit of the cloud-based Identity Based Encryption (IBE) method is that there is no need for the sensor to interact with the Key Distribution Center (KDC) to generate a public key, as the sender is already aware of the receiver identifier. The earlier suggested attribute-based encryption method solves problems with cloud-based IBE approaches. The main policy of Attribute Based Encryption (ABE) is connected with sensor identification as per traditional ABE system. The general method of attribute-based encryption system involves four significant algorithms to be performed, namely: Setup, KeyGen, Encryption, and Decryption.

All the traditional cryptographic systems depend on both mathematical methods and unproven computational limitations. The above group of algorithms is generally implemented over an unsecure medium on applications involving the sharing of secret messages. The big issue that arises in conventional cryptographic algorithms is the key distribution problem. It

has the responsibility of providing its customers with vast storage space and quick computing mechanism via the internet. The data owners in cloud computing mostly transmit messages to the server. We can also say that, in other words, data owners upload their data into the cloud. In addition to cloud's numerous benefits, there are certain privacy issues. Vast amounts of sensitive information exists in the outsourced data. Therefore you need to encrypt this sensitive information before uploading. These data need to be used properly, too. Searchable encryption scheme is introduced in the subsequent time in order to perform basic search operation on encrypted cloud data. In the above approach, the data owner is responsible for encrypting all the documents along with the associated keywords before uploading them to the cloud. At the same time the search methodology is responsible for producing the encrypted trapdoor which includes numbers of different keywords[6].

KP-ABE includes numbers of various attributes that must match multiple access structures. By contrast, CP-ABE is a specific access structure that matches multiple attribute sets. In the case of various access control applications the CP-ABE technique is much preferable. Both the CP-ABE and KP-ABE techniques are appropriate for implementation during the keyword search process. Customers are permitted to choose their methods according to their situation. The cloud computing provides various services according to the demand of the customers through resource rearrangement. It is responsible for relieving the users ' excess overload in order to manage various information systems. Users are required to outsource the data into a heterogeneous environment within the cloud environment. This environment isn't always customer controlled. With IoT's advancement, vast amounts of data are generated and transmitted over the network. The process of data processing, analytics, and data mining is considered to be three significant processes to assist a party in making profits from both the own data and the data from different parties. Cloud computing allows users access internet services online at any time from anywhere[7]. It can be done without thinking about concerns related to technological or physical repair and control of the original capital. To several, however, the cloud computing technology concept remains like a vague notion. Therefore, if cloud computing is to achieve its potential, the factors that can affect its adoption in various organizations need to be clearly understood. As many companies know that cloud computing is quickly becoming a key component of long-term IT plans with less costs and reduced time-consuming efforts[8]. We are getting more interested in moving their systems to the cloud and finding more ways to exploit those systems in real time to ensure that the cloud computing model has significant benefits. It allows companies from every place to access cloud-based services and encourages better communication between various organizations. Nevertheless, several companies have been reluctant to hop on the cloud solution due to the lack of appropriate privacy and protection techniques. Cloud's benefits are not limited to consumers or individuals but apply to other enterprises, governments and private institutions. Given security and privacy concerns caused by leveraging cloud benefits, which can delay performance and hamper success for many users, cloud components are common and critical. Security problems should be analyzed on a wide scale to find appropriate solutions to improve cloud adoption and performance. Cloud service providers allow users to store their data in the cloud, without worrying about user data integrity. Users can upload critical data to cloud servers and access data whenever and wherever they are.

Users main concern is that they lose control of their outsourced cloud data. Consequently, users need evidence that their data is stored in the cloud. Cloud storage does not use methods which may help protect consumer data privacy. Image integrity is considered to be one of the most important components of any system; when image integrity deals with a single database, it is responsible for the database's protection or survival through a set of restrictions.

In distributed systems, this situation is relatively different as these systems include and handle multiple applications and databases, creating security or privacy concerns. We will also seek to find different ways of preventing these problems. Cloud computing image integrity means maintaining the credibility of a remote image that is stored in insecure cloud servers. In this case, a protocol is used to gain ownership of the images in the cloud, and this protocol must ensure that the images stored in the cloud by the actual user are not changed or modified by any archive; therefore, the quality of the images is assumed to be authoritative. This authentication scheme prevents any cloud storage archive from transferring or modifying images without the image owner's permission. Medical images outsourced in the cloud will help the information required for a health system, physicians and patients needing management in many branch hospitals, thus minimizing the knowledge and computing resources used in the hospital. In addition, the obtainable medical appliances can be regenerated as medical terminal units to be more resourceful and low-cost[9].

Verification of the integrity is used to check the behavior of the node and its changes on the communication data. Traditional algorithms for verifying integrity are hard to avoid attacks and collisions in static and dynamic cloud networks. For vibrant cloud networks these algorithms are also not very effective for large volume information. A huge amount of study papers on cryptographic integrity features were introduced to authenticate communication information in cloud networks. During cloud data communication the authentication model is used to validate each cloud client. In the literature traditional authentication models were proposed to authenticate each cloud client in the cloud network. These authentication models are basically time-consuming and impracticable for large cloud networks. The main problems in these models include: limited data size, difficult to generate value for integrity of variable size and difficult to generate a dynamic hash value on wireless networks of large size.

2.Related Works

Rady, suggested a new method for the detection of attacks. This method is entirely based on a scheme for ant colony optimisation[10]. One of the most prevalent issues in the independent authentication method is the hole in the safety loop. Pheromone activity is responsible for representing the amount of node confidence over the entire certificate sequence. The primary limitation of this model is to improve the general scalability of the network by increasing numbers of nodes. Furthermore, this method can be modified and expanded to recognize the chain of certificates composed of Sybil nodes multi-identity.

Wei et.al, proposed a cryptographic method for protecting information from cloud path planning within restricted cloud networks. They created model CP-ABE. This model focuses on the basic concept of cipher text that is related to the access control system. Here, the features include hidden keys too. The method of decryption is allowed when the respective properties fulfil their desired access strategy[11]. The entire operating method of the CP-ABE model is completely reversed from earlier KP-ABE created. Because the CP-ABE method is more versatile than other attribute-based encryption methods, it can be applied readily in a wide variety of apps. It has been unable, according to the KP-ABE strategy, to regulate who will decrypt the cipher text that is deemed to be the main restriction of that model. CP-ABE tried to resolve the above-mentioned problem of KP-ABE approach effectively. Because of this function, CP-ABE method can be effectively implemented in multiple applications in the actual globe. The model proposed above also has a severe drawback which restricts this scheme to be applied in business scenarios. It is not fit to be implemented in enterprise applications due to the less flexible nature of this model along with very low efficiency rates. Single set attributes are needed for successful execution during the decryption process[12]. Users are meant to select a specific attribute or a set of attributes from that set of attributes. Further research efforts were made to resolve the CP-ABE approach problem identified. CP-ASBE (Cipher Text Policy Attribute Set Based Encryption) is recognized as a perfect solution among all the solutions developed.

Fan et.al, proposed the introduction of a novel model where CSP distributes the full job queue to a shared cloud setting and a mutual personal asset for greater profit. It provides the load balancing method which is based on job reproduction. It divides the entire queue into sub-cloud, distributing it to all sub-clouds. Every subcloud assigned VM starts handling the task and sends messages to each other via VM if someone finishes prematurely. So, everyone is stopping handling and dequeuing the work from their work queues pooling scheme. In this approach a lot of handling energy is lost, and the implementation time is more than any other algorithm13].

Ferretti et.al, offers cloud service providers a Dynamic Resource Allocator (DRA). The skewness strategy being proposed is used to avoid overloading by having different workloads. It enhances the scheduling of the server resources by calculating diversity in the server's resource utilization. There are several resources in the server that consumed uneven resource, the skewness strategy is used to calculate such situation so that the load balancing can be done in which we can find skew values for all running VMs and can predict the future loading. In this strategy, VM migration can be done for the realization of the system's overload condition and can also be done with the strategy of load prediction.Significant research interest in cryptographic hash functions has been observed in recent years, particularly after the common attacks against Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) in 2005. Cryptographic hash functions are also referred to as Message Digest functions and have various information security applications, including digital signatures, message authentication code. Cryptographic hash functions (image, documents) are used to extract a fixed-length bit string from a file.

A cryptographic hash function is an algorithm and math function that transforms a numerical input value into another numerical value compressed. Message M (arbitrary values) input to the hash function is returned (produced) by a hash function, and is hash values (fixed length) that are often small in size. The following picture illustrates the hash function: Most cryptographic hash functions are designed to take a string of any length as input and generate a hash value of a fixed length. There are many applications of Cryptographic hash function. The honesty checking is one of its most significant applications. Some changes in the input data will change the resulting hash value to any bit. So modifying just one bit of the input would drastically change the output. Therefore, hashes are useful in detecting any alteration in a data object, such as a document, or various manipulations of multimedia data and digital images, such as compression, enhancement, cropping and scaling[15].The use of encryption technologies is not limited to the implementation of data (texts).Main advances in the use of hash functions with image encryption or other multimedia protection and indexing applications have recently attracted considerable attention.A key feature of modern cryptographic hashing algorithms, such as MD5 and SHA-1, is that they are reactive to the message, i.e. the image hash function will then accept changes in the visual domain and generate hash values based on visual features of the image. Cloud computing tools can be distributed on demand rapidly and efficiently and easily scaled up with all the required processes, services and applications, such as the allocation and usage model. NIST defines five key elements, three cloud service models and four cloud delivery models, as shown in Figure 1. In many companies, the use of cloud computing is increasingly growing, and is a dominant model for business systems. In recent years, many data privacy related reports have been outward given the security measures implemented by service providers[16].

Some of the effective protection mechanisms the CSP (Cloud Service Provider) uses to ensure data security for consumers is encryption of the data stored in the cloud, and key security is the possible vulnerability of this process. Many cloud services, for example, hold a backup of the encryption key and conceal this information from their clients, they can theoretically decrypt and view all the data stored on their servers, such as Apple, which has a program called "iMessage," which manages text messages in cloud. We ensure that all messages are encrypted end-to-end but do not inform their clients that they are legally allowed to hold a copy of the key[14]. CSPs encryption process allows the clients to trust the CSPs entirely as they control the keys. To ensure the security of the cloud's sensitive and confidential data, some research suggests that the clients encrypt the data until it is stored in the cloud. But this solution requires an efficient and stable key management solution in the customer's obligation, as they may lose the data forever in the event of key loss[15]. In order to secure data storage and processing, we need a powerful cryptographic technique that satisfies certain requirements, for example, to guarantee a fair period for the processing of any request submitted by the client and a minimum size of encrypted data that will be stored on the Cloud server and that allows for distant calculations on encrypted data without decrypting it. Yanet Al[16] are proposing to crypt data before sending it to the cloud using a Homomorphic Encryption-based cryptosystem that allows encrypted data to be computed without decryption, this technique avoids the question of supplying the cloud provider with

the encryption key to perform the necessary calculations. The proposed fully homomorphic encryption takes more processing time and memory than the same unencrypted data operations, it runs slow because of the need for faster, completely homomorphic encryption schemes.

Zhouet Al[17] suggests a parallel processing of Gentry's encryption, which dispatches and separates FHE encrypted data operations between a variety of processing engines and shows that this implementation increases performance better than computations on a single node. In order to maximize performance, many cloud environments do not encrypt their data; they store it in plain text on the disk. This is a significant threat to critical data, a provider's rogue employee or unauthorized users of the operating system may access confidential information by inspecting the contents of device files contained in the disk. Some of the most significant driving factors behind moving to the cloud service is high availability of infrastructure, data, and applications. When deciding among private, public or hybrid cloud vendors as well as in the delivery models, it is the primary decision factor. Hence the provision of information in the service level agreement should be emphasized by businesses to ensure access to their data[18].

Garg et Al[19] provide examples of attacks that that impact the availability of data such as Malware Injection Attack, in which the hacker inserts a malicious code into the data transmitted between cloud provider and client.As a potential outcome of this attack, the cloud service could be inaccessible before the maliciously implemented job is complete. Another attack that may have a detrimental effect on connectivity is Distributed Denial of Service (DDoS) attack in which a legitimate user and partner is robbed of the services and resources they would usually expect to access by consuming all usable bandwidth. This attack has a major effect on business operations, such as loss of income opportunities, reduced profitability or damage to the image of the company. To reduce this risk and provide resistance to the failure or misuse of sensitive data on cloud providers, and also provide many possible benefits, such as high availability, reliability, fault tolerance, continuity of business and recovery from disasters, various ideas have been suggested that apply the so-called "cloud of clouds" or, in other words, "interclouds" or "multi-cloud" strategy.

Multi cloud solution is a cloud storage architecture that uses a variety of diverse commercial cloud storage services to create a virtual cloud storage network. The data to be stored is thus split into separate blocks and redundantly spread to different cloud storage providers. There are two ways to go about redundancy. The first is to duplicate the data naively to many providers by storing a full copy of a file on each provider and the second way is to scatter properly encoded data in such a way that only a certain file fragment threshold is needed to reconstruct a file. Cloud providers are able to exploit consumer data without having to rely entirely on it. Many surveys of potential cloud adopters indicate that protection and privacy are the key concerns that impede its adoption. The issue is that while data can be transmitted in encrypted form to and from the data center of a cloud provider, the servers that control a cloud can not do any work on it this way. Therefore the hidden key to decrypt the data will be exchanged with the provider if the company wishes to conduct calculations on its data in the cloud. Sharing the key will require access to the data by cloud

provider. Homomorphic encryption is the answer to that question. The client will have executable code given to the cloud to allow it to operate on the data without decrypting it. The output is returned to the already encrypted device. Therefore, because the client is the sole holder of the secret key, nobody else can decrypt data or outcomes. From 2008 to now, cloud computing has been developed from different technologies and it is being put to work in a number of solutions and services that have led many businesses and researchers to propose, test and introduce innovative cloud computing systems. The literature review seeks to cover all related high quality research literature[20].

In [21] Li, et al proposed a method for (KASE) user revocation in cloud storage, any customer can selectively share group of selected documents with a group of selected customers in this proposed framework, as well as revoke the customer in the framework. Forward secrecy and backward secrecy are used for the main updating of cloud storage in user revocation. The mean of forward confidentiality used when a new party joins to the group to warn the community of the new member's aggregate. Although the mean of backward confidentiality used when any customer leaves the party, the aggregate key needs to be changed on the server and the new aggregate key needs to be reported to group members. Business requirements are met by IoT while novel services are implemented based on real time data. IoT is the connection between the physical and the virtual worlds of life. Connectivity between these items may not be private property and is available at a low cost to all. Because privacy security is important, the use of blockchain technology will protect IoT from malicious attacks and fraud. One of the major benefits of using blockchain-based user preferences management scheme is that it plays an significant role in resolving conflicts between users and IoT service providers[22]. The unchangeable, undeletable, distributed, and irreversible existence of blockchain makes it ideal for decentralized identity management and distributed credential storage. Such blockchain properties embed potential for enhancing security. Using IoT blockchain allows for a genuine decentralized market to be established[23]. The absence of a central point in the blockchain-based systems avoids failure that sometimes comes from a central point, thus providing a complete and clear factual historical transaction log. By ensuring that each party is responsible for its positions in the entire IoT transaction, Blockchain avoids disputes. More protection may be provided to a device as the network size increases exponentially with authentication being carried out at no cost. In addition, blockchain is capable of playing a major role in tracking the origins of vulnerabilities and solving the security vulnerability issue. Blockchain-based identity and access management systems will tackle major IoT security issues such as the IP spoofing challenges.

Ultimately, the Internet of Things (IoT) dream is to make sure existing devices are autonomous and smart. Technology advances transform the dream into practice, but some challenges need to be addressed, especially in the security domain, such as authentication and reliability of the data. Thus, in the era of huge information source, it is necessary to make it trustworthy for IoT future potentials. In mission-critical environments, IoT technologies are used in areas such as data storage, sensing, identity administration, administration, smart living technologies, timestamping services, mobile crowd sensing, intelligent transport systems, and security. By combining blockchain with IoT, several researchers have made

attempts to develop these kinds of application. This integration has the objective of improving the authentication process. Some of these studies which have combined blockchain with IoT will be reviewed in the next section. The applications are categorized according to their categories[24].

The Blockchain is a innovation which the world looked forward to after the emergence of the Internet. This is an innovative and creative path-breaking and irrefutable innovation by none other than the founder by Bitcoins. Undeniable, Satoshi Nakamoto created Blockchains to ensure the accounting of the Bitcoins, and was thus a subsystem of the Bitcoin setting. Blockchains would have been the core of the Bitcoins accounting and audit trail and its support network. Compared to the Bitcoins, which is just a part of the Cryptocurrency scheme, it has now evolved as growing and more appropriate[25].

The Blockchains consist of their nodes known as lifeline. Blockchains may be known as a database node network. Nodes verify, and distribute the transaction between two parties. When the transaction is approved it is added to the Blockchain chain of transactions. Different tandem nodes build a very efficient monitor and built-in network for the entire Blockchain ecosystem. Each node, however small or big, is an independent Blockchain system administrator. The node is a volunteer organization that has joined the ecosystem to receive Bitcoins in the form of incentives for its ability to decipher the difficult algorithm leading to the transaction being validated and reported as a block[26].

Nodes are involved in Bitcoins mining- a method that is a reward for the transaction being verified. The mining method is a race for earning Bitcoins between various codes that employ superfast and supercomputers to crack the complicated algorithm that hashed the transaction. The node that is first able to split it is entitled to reward. Therefore several nodes attempt to beat each other in a bid to win rewards. Consequently the Blockchain is a breathing network that never sleeps. Bitcoin mining is one of the features that can be added to the Blockchains[27].

In addition to the Bitcoins, other such Cryptocurrencies which count about 700 use the Blockchain infrastructure to ensure its transaction's stability and sanctity. Besides this, Blockchains are now being used by many other developers around the world in designing their framework or operating their systems. The Blockchain is de-centralized and independent of any power. Any activity occurring in their environment is not regulated or managed by any agency or authority. It's up on the internet. Many organisations have started to see the significance and applications of the Blockchains, even though under an agency. For example, stock exchanges have started tracking the transactions on Blockchains, and this has meant that the transactions that took place on a specific exchange are completely monitored and reviewed. Land records are documented on the Blockchains, and hence any register held by the State is gradually transferred to the Blockchains. It is shown that records over the Bitcoin blockchain Blockchains are handled by a worldwide network of machines that help monitor their transactions.Therefore Bitcoins are handled by node network and not by any entity. It is the fundamental concept of decentralization, which implies peer-to-peer controlled network. Such nodes 'mass communication around the world makes it a true network of decentralization. The program is run by individuals, not by governments and organizations.

Blockchains 'second-largest users are Developers. During their initial period of existence, startups operate on limited margins and Blockchains will cut off the middlemen for startups. So both of these areas follow Blockchains massively. This has helped companies since personal computing has made them directly available to consumers through a Visual User Interface introduction. Individuals have followed the GUI or Visual User Interface, as it has done away with the text-based interface. In the introduction of Blockchains, an individual's personal data can be pooled and the individual's data would belong. He must allow any person or organization access to the data and to the extent required, and also define the access time limit. Being a central repository where data is stored safely on a network, the Blockchain environment eliminates the possibility that data will be centrally stored and managed by some entity. Since the data is not centrally processed the possibility of accessing the data is minimized. Existing data are usually stored using the username, password protection, and access system. The Blockchain uses the more efficient, 256-bit encryption[28].

The encryption is based on a combination of public and private keys. A public key is typically a long and randomly generated number string, which is the user's address on the Blockchain network. On this public key network which is also called the wallet, the user can obtain and store information and Bitcoins. A private key is a password for accessing the network with the public key. Therefore the network of public key wallets can only be accessed or used with the private key. Therefore, blockchains operate on two key features rather than one key access function, and are more stable. Nevertheless, it should be noted that there is no way to secure the data or Bitcoins on the public key wallet until the private key is compromised.

The public-private key network provides access for the user to share and access the data encrypted therein through the Blockchain. This is available to anyone who feels the same. Then the double level of security is applicable to the users on the internet. The access comes with several riders that can be granted to the user, i.e. the user can be granted restricted or time-bound access as needed. It isn't usually visible on other internet networks. Many of the citizens already use this Bitcoins transaction network over the Blockchain protocol.

Most of the merchant banker, like Goldman Sachs, is of the opinion that Blockchains hold great future in the clearing and settlement banking system, and will also provide significant transaction cost savings. It is estimated that the banking industry will save approx. $6 billion on the transaction charges.

The Blockchain technology has given the startups a drive to build values using digital knowledge authentication. The Indian Unique Identification Authority's Aadhar card is one such example where the use of Blockchain will allow for limited authentication. Think how much data can be limited to the person to whom the data is being given. In addition to the digital information industry, the industry of smart contracts using Blockchains is fast catching up in the business world. Smart contracts are signed digitally without two parties to it meeting. Blockchains help to represent agreements and contracts in such a way that they will be executed automatically when defined terms are satisfied in the contract. Smart contracts are dealt with over the Ethereum which is also an open source Blockchain project which was

specifically designed to meet the possibility of unique output contracts. It is a path-breaking technology that can alter the way the contracts are executed by the planet. To offer an example, smart contracts can be configured to perform a specific task such as buying a share or deriving if the same meets the investment or purchase requirements set, and vice versa. This may also be configured to unlock the payment on the sale of shares or options using such a contract to conduct the transaction. Thus, automated buying / sales and payments can be configured over the Blockchain allowed by Ethereum[29].

3.Proposed Model

In the proposed model, cloud-based block chain security framework is designed and implemented on the e-governance applications in order to provide strong security against the third-party attacks. The overall framework of the proposed model is represented in figure 1. In the figure 1, each transaction of the e-governance datasets is given to block chain framework for block security. Here, security blocks are used to compute the hash of the input transaction and encryption. Current block hash and previous block hash values are encoded to provide strong security to the block chain framework as shown in figure 2.

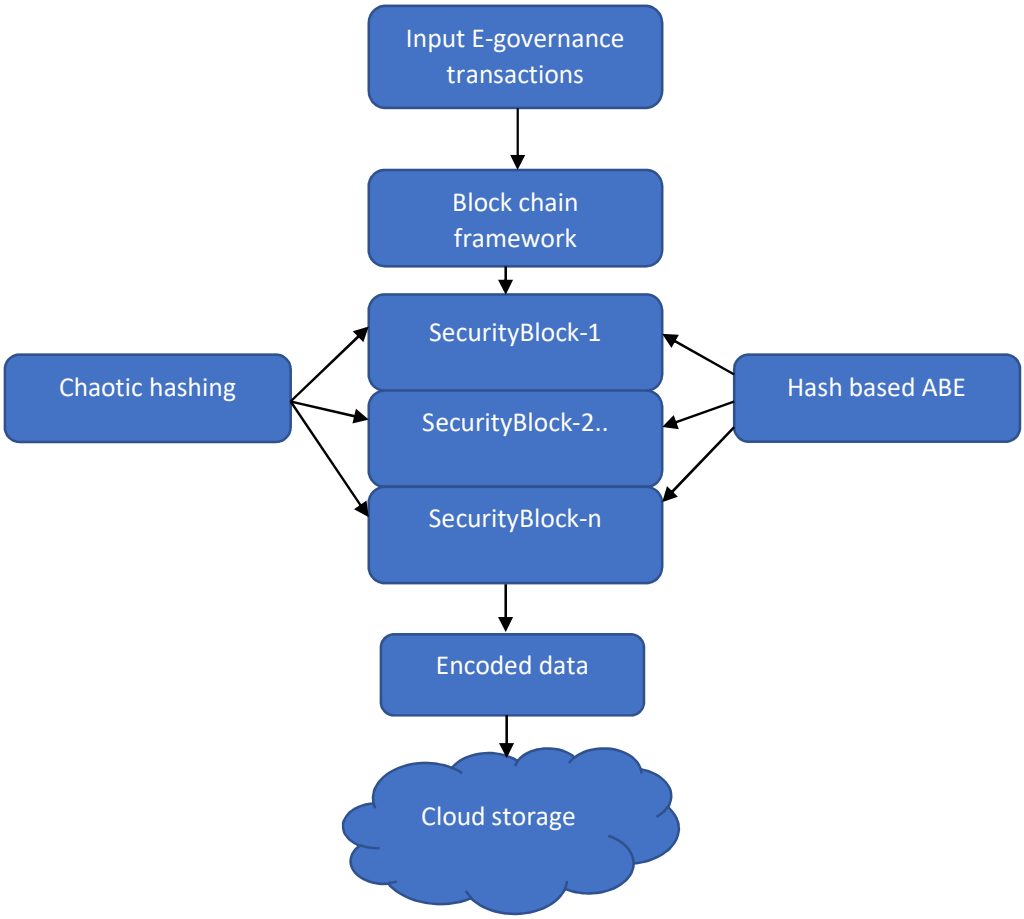

Figure 1: Overall Proposed Framework

The current encoded data of each transaction is stored in the cloud server for integrity verification process. In the proposed work, a hybrid non-linear chaotic integrity based encryption model is implemented on the real-time e-governance transactions for block chain framework. In this work, , e-governance datasets are taken from the Andhra Pradesh NREGES real-time web application for block chain framework.

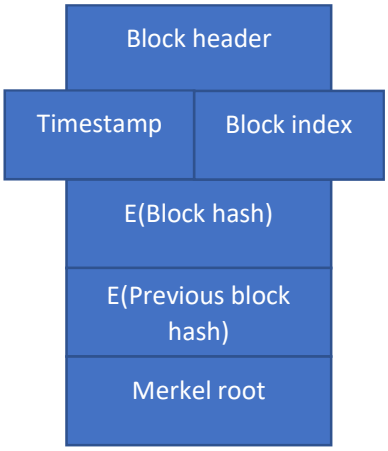

Figure 2: Structure of Security Block

Hyper-chaotic systems with over one positive exponent of Lyapunov generally have more complex structure and dynamic behaviours than chaotic systems with a single positive exponent of Lyapunov. In the figure 2, timestamp, block index number, encryption of block hash, encryption of previous block hash and merkel root information are encapsulated in a single block.

Bilinear Map

The Bilinar map is the mapping of one cyclic group R_1 to the another cyclic group R_2 and it is given as:

$$e: R_1 \times R_2 \rightarrow R_t$$

Such that:

$$\forall u \in R_1, \forall v \in R_2, \forall a, b \in \mathbb{Z}: e(u^a, v^b) = e(u, v)^{ab}$$

Process hash block

In the proposed chaotic piece wise non-linear chaotic function (PNLCF), different randomization parameters are used to generate a unique chaotic number for the

permutation matrix generation. The extended piece wise non-linear chaotic function is given as

$$PNLCF(n)= m1.\frac{k(n+1)}{256} + m2.|\sin(k(n+1))|^2 + m3.|\sin((n+1))|.|\cos(k(n+1))|^2 + m4.|\sin(n+1)|.|\sin(k(n+1))|^3 + m5.|\sin(k(n+1))| + m6.(1-PNLCF(n-1)) + m7.(1-PNLCF(n-1)^3)$$

Here r1…r7 are the random number (0,1).

In this non-linear chaotic function, Q and R represent the dynamic permutation matrices. These matrices are generate using the PNLCF function.

For each byte in P[i]

Do

$$R_1 = SK^T.\ [R.\ MaxEigen(SK).\ (MaxCoeffient(Poly(SK)))]$$

$$R_2 = \left(\frac{[Q.SumofSquares(SK).det(SK)]}{(\sum SK[i])}\right)$$

$$R_3 = \sum PNLCF(n) * Eigen(Q.R)$$

$$H[i] = R_1 \oplus R_2 \oplus R_3$$

Done

Dynamic Chaotic CP-ABE Encryption Model:

Phase1: Cloud setup: In this cloud setup phase, each cloud node initializes its own cyclic group parameters and chaotic

Let G_1, G_2, Z_p are cyclic group pairing elements.

$$Pubk = \{H_{4096}(G_1), H_{4096}(G_2), g^{H_{4096}(Z_r)}\}$$

$$Mk = \{H_{4096}(Z_r), g^{H_{4096}(Z_r)}\}$$

Phase 2: Cloud data encryption:

Step 1: Key generation

Select large numbers p,q,α,β.

Compute n=p.q

ns=n*n;

$g=ns^{-1} \bmod(\alpha \bmod(\beta))$

$$\lambda = \frac{(p-1)(q-1)}{\gcd((p-1),(q-1))}$$

Step 2: Encryption phase

m=input value, r:random number

Cipher value $m_1' = (g^{m_1'} \bmod(ns).r^n \bmod(ns)) \bmod(ns)$

Cipher value $m_2' = (g^{m_2'} \bmod(ns).r^n \bmod(ns)) \bmod(ns)$

Step3 : Additive and multiplicative homomorphic

Additive :

$sumhomo = (m_1' + m_2') \bmod(n)$

Multiplicative :

$prod\ hom\ o = (m_1' * m_2') \bmod(ns)$

$$\text{Ciphertext CB[i]}=\{Atree, C, R_n^{\,k} (\bmod(s).R^P \bmod(e^Q)).\bmod(e^Q)\}$$

Phase 3: Cloud Key Generation Phase : In this phase,

$$Sk = \{Attlist, g, g.H_{4096}(mediadata), g^{H_{4096}(Z_r)}\}$$

Phase 4: Cloud key Decryption: In this phase, attribute list, cipher text and cloud integrity value are taken as input in order to decrypt the cloud data using the access tree structure.

Decryption phase

c:cipher value

$u=((g^{\lambda} \bmod(ns)-1)/n)^{-1} \bmod(n)$

Decryption value:=$(c^{\lambda} \bmod(ns)-1)/((n*u) \bmod(n))$

4. Experimental results

Experimental results are simulated in JAVA IDE tool. In the experimental results different types of input datasets are taken as training data for integrity computation and encryption process. In the proposed framework, different types of integrity algorithms are applied on the input files to test the integrity value and its hash bit change .

Table 1: Integrity value of different training datasets

File Name :nasa-category.json
a123ef21b3a9d173a2a2e07fab8fa4cdd8e49563
File Name :nasa-tag.json

3895ac8d460d4a4f59146466771a02c6def855dd

File Name :seismo-index.json

31907c3d4f7231e1200b65620b29b2f13f5eb135

File Name :seismo-index.xml

aaa789dc4a530be38411ff7eb41ad15ace682ead

File Name :seismo-station.json

403ccee133e100a51e170a6578e1f1e7c7a890a9

File Name :seismo-station.xml

203f0bdf10a3753184ba971f14a293756ab80d71

File Name :usajobs-big.json

43bdbe99b7882dd5c4db564a6f14562eb0a9dffb

File Name :usajobs-big.xml

b07452af0da83f781483ba9029d5f706e129fa09

File Name :usajobs-small.json

0199253cd8f37c88b32dc0b0b18974755cb7906f

File Name :usajobs-small.xml

103870b79552348f05f9e6cbc0456f25dfadc3de

File Name :weather-big.json

7d83d5bf36681274e1f0db67e16f6c6124f52837

File Name :weather-big.xml

e1f0ab81b780cd6aa6bd8987745308d7c4628d37

File Name :weather-small.json

4e88e9659616f00abfd94198eb2b7ccd0c9aa8f3

File Name :weather-small.xml

e5d1d154e75e22f7c5307b07423137ff98b6f7f4

ripemd256 ALGORITHM

File Name :angel-big.json

409ef06dbdc342ff25a6fba9d4424be9f87ed53cbb0b988061a3f7b24e1d47c1

File Name :angel-search.json

0c5de9b3bfeb1fc8d27b006edb90bddb3cc8e32f0e820139b651ae5aebd7fe90

File Name :angel-startups.json

40eaa717ffe026fc05923631d7e55a9b740c7081f91cd659206aacb4505d0247

File Name :angel-status.json

53852d5c0305e317048cfe4c66540784f82988b55cf29bf830ec64e45a90e888

File Name :get_data.sh

f187ba84a8c1c23d42303344a6590181eb968d5cbbc10b9b11dab28baabd337e

File Name :nasa-big.json

5cfbc104aab2bce0cb912d92d318c5f5fd89783a61c0acf6e2a0aecddbc601f2

File Name :nasa-category.json

23a3d82ac69f820a75a77f381b75c2f3fc7e5f6468af1839a6f5954fb939d790

File Name :nasa-tag.json

b0dc102d7d9e0864475c1dd5783b9b11e0c9451e706065f3a46f70db48dece83

File Name :seismo-index.json

d81f73765e2f07114db494edb252af61295e62c1df5c9ce4bc75cac2b654e710

File Name :seismo-index.xml

aad1356f7b78fa2d72e9b473273cd24dd613e7baf86f3a033b69cf787e832b5f

File Name :seismo-station.json

64a2f294baefb786ec56f9ed91ab431d6c1b27c57f99712077df6b43028ef2a0

File Name :seismo-station.xml

80c1ff3018bdceb13845d82745197216c54f73dce8ce32424d99738676844bdd

File Name :usajobs-big.json

30b093f15133448ab2fb44926d0b3c79411b6cd5950e5c3226b13c7be34b6d3d

File Name :usajobs-big.xml

af2c1d1f813793bcc352a23e76dc9d9121b24a0e3ab918f2c82f75eb0d2f095a

File Name :usajobs-small.json

8dc62a3be337ac6fd1d7aa6ea4b3711bb375ff8df888698b9a9b9e7f212aa85a

File Name :usajobs-small.xml

ae226f9219c5b688ae94735a569d4c24faa5ca886343261100a238385816b407

File Name :weather-big.json

beeb6708064f9f15f7359abb78226fdb1d20e07d262de81cf8eafb279a936126

File Name :weather-big.xml

fa07f8d563e525bde8b4883e6507ce3732b65d73472c8bd657d5b928b5f8d331

File Name :weather-small.json

641bc1b9b5352bda0c2bc5f71eda2b15127505e27f789ade2a43db23a9193347

File Name :weather-small.xml

23163b224456aa04842a2e6b287c15b4b90a3f8bdc476564f08d5cc9e388efbe

ripemd320 ALGORITHM

File Name :angel-big.json

5a9c4ed5978cf5538ffad0ca1b77adc1a4ff42b799afb8b6ce9288f0504a3584d84aaab6ee5b49f1

File Name :angel-search.json

6f8fc45146d3de1d485c4a01ab804fba4ee8e5724227c1d03ebe1e27e61842315d87ac0073f30e67

File Name :angel-startups.json

a5e2b1b45ec4b91baa89b4b76cb99edcc621c081b2051b6d267896ac57de0ea61e7d9c44eac89e7f

File Name :angel-status.json

12d0524bb61997cf9d3e64eb2132ebd60210d958d4b4eb4164b811261e4d7343e53f120ecea24f01

File Name :get_data.sh

84b08dfd21f6e406541956cf8cf7132c8f23eca3688f20fa0ae07b6c1d52e2dac57c58f534df2092

File Name :nasa-big.json

fecde53c5861e1580dd4537bb0ad0c4694ead554d8273187403529a5757fbc128c1dd9f705530e8c

File Name :nasa-category.json

0fd751543eafa2bd45a3f041e2b3d203fbb1c0e45b09109c01d9b75ad9dd2a2218e763c2e9726888

File Name :nasa-tag.json

d887e5ac67d99fa1f8b6996a3506209afef752b6bc155da633325c88a03c8d4fdeca31d20aea7995

File Name :seismo-index.json

f9a1bca61c631b5f7e28c2e0066770b97c07424ea9066f7ad99cba157c1859d1dbdc01d073a3bacf

File Name :seismo-index.xml

76f7359270b97d16e6834f5cb041a37144ef307fa0d0ca3ad88317a20a7fcdeb4f1647b610741ecb

File Name :seismo-station.json

42f59d22762902b3f62d7f18ca4d4e7611b7a13e138397fe18203139194b74636e17e27c8c39bd3d

File Name :seismo-station.xml
7d8b1d8651d67ad02776a3f805f3e8816d5f72981a53f798a217d100dab3e93cbbf84c5265d505d2
File Name :usajobs-big.json
72fcfec20de6e2dc7e7ca0c39f0f12a98cd4f9dfaf559b732f5af3838117c7f200f64b5377e6553e
File Name :usajobs-big.xml
769725d051c4687174e2f9754506eb883cfafc289eb500e27375b7a2d466564d18451f9e5811b583
File Name :usajobs-small.json
d75cd4a9da3573256859615b4b606ee187ebc6e11de88fe3dacf250cb94faa90cba8bab84c2368c3
File Name :usajobs-small.xml
83cc61cb69d6a156cb4ef71e043be44277c5ed43171b7e3f8d820ba17f284fdeabc1d5128d1155c3
File Name :weather-big.json
32038f2d58694333f49159b215382ca0eaecd9e46877046f654c8940c00ced348d4daf6e8a8ea42a
File Name :weather-big.xml
f34d632a187f2db780873d334a147790ceb2458e96bd386f0e1bc164191d04357378c45001ad8e55
File Name :weather-small.json
945ee6f68ec4ce6116b2aab48f9257af2d57fec4fcaca7db9e88b1718949bdfde6b5649b82ca3235
File Name :angel-big.json
b3598e7effedb3a836ab54a8959c9350dc085780eafaf39d1f800313216e92102dea1f25f189399b1fedbaf68d63bbb5e5c6e377a59c8aeec3fe75e3abce0577
File Name :angel-search.json
c685aa29b70cef6a85b39ad2afef71636207cc61a9c1bb2debb9b745043c7157f510db1b6e82d9e15256ab7128d9479284624d42518328100f766076f1c65769
File Name :angel-startups.json
d74c1215f779d6c9fd71bfb992f52c9b29a57847f2417ea8b8519604862e99e8964131cf21c266f16e35146284dad526a0eef74cbb2c0bfdd532dec967f18cd4
File Name :angel-status.json

c8cbc7bab8b231db7cbeb65bb70117436f6df52917e589284ec7ee563cf481aefdafed8fd1381d1
1af1a1ce1ce54bc5f9865332b738c8c5d0d1e00e1041ccded
File Name :get_data.sh
fd64582ca7d0892396b8a58966b2600ac64ba44dcd2220f557879a2f3f3436bb9d975b16ea17f6
77046a66436a1a955e47a39ebe1f20895938f315e051ceb24b
File Name :nasa-big.json
e3da44cf6b0b3d6529277a92c2262a3d8845f34ba5205c3091c44cec13622aba32f3af9a8ce660
fc79008880664b1d5ec4b723eedbd858219e96389a5de50f14
File Name :nasa-category.json
5cacee46e899a507c34ffedddad2216d8849cd153700fcd1b41d81ee1f0fbac8fafb28bf0d8c428
df185e0cd933122cb20b04f544dffef7716f620aa45c3bf62
File Name :nasa-tag.json
ead3d5f4cf168ec386570bf3597764aa772f048d78de926dc109575040e7c9bbc8200195175ca0
74b31faaab8c943186aac8a74780973adb610efb8426e43a79
File Name :seismo-index.json
1b09a38dd84a4f66c5caa112b7b152f54bd0a3d6a73f2fa1601d6c94192c26bfd5081103076ba5
f8e4586b8bcb6e2c5e7977e4f5328c01f26b0540993d1c5122
File Name :seismo-index.xml
4f05751499bed43071554a0b8d5aac06032f7af21055c2c0f52ea6e073e750cbb2fd968f2ffb122
8ba871147166f11f4de8565612f524cd49d3187403d16a1f1
File Name :seismo-station.json
14c8e9a5ac881e8fcf40bb864c16ba589b1544fb85ee76abab61f4c1f4b4d1a6096e395f2ecd911
8213b3842e1daf45069bd073f77602c1a7207e047ff7254b4
File Name :seismo-station.xml
b608da28e97caeb24e8e7d43ec479c4b601d3ac5de3fb75ba3bb171df2c1a9f58dcb9376231c0e
9bc6232954d65ab3b72b5c1d0331846cbb68b633c44804b6a1
File Name :usajobs-big.json
e127c0be9a6d1702c417dee5f84acfa1e15532ee5b45fb2e919b162b2e191bf601fafe1643d3f92
52ff0d243d92632b84ba6e37236bb5cc4bbeba4b55ca7de07
File Name :usajobs-big.xml
1906dc5f852ebf12ae8ecc590267c476f8d2041603a6d8d26db08d6445bf0bf39653cd234c2de0
c072225abf98c4cbfb766dfdc0538f9ae98902731b75b74ca3
File Name :usajobs-small.json

071d757237bb796ebd898cb1893e07119cd00668ffcce5ea6c163916d5bc86d80371237d3b98c
e8d68da7f9272b1953034beb7186bdd3e223fe55a98da26eaa8

Proposed Model

File Name :angel-big.json

66cd187775925a7c7f92e4499b0d14342d51fa246a4e43797fc431d9d3248fe234ec874eccc5a7
9871dd07e552aaf38779a1bd47ad6b555e716a722a38030614e43442ad0de7a47e17ceae19135
2a49706287ab3a36e754ff806c476d941d14e906ca373384ceb573904d0965b62d750d14c0638
3ef706b0768f49ed75359f0a1fb44fcb138c51763acf2c09006a04453217188f886346e8950376
9059bbe4d64b081dbda60f37a583dd6b7e83274098b799534a46c4e836cfa41946898998dc2b8
07dadc6db25d8c86145635afa7c12dbdf92ffc469bb5d49eb154253dab2d4b22653d90452bfea5
7c7005f0b610b5244e8e50fb385467bd7389ad22af1c2cb4007791b420dbde60fb675b748d433
60fdb5bdb3409f0c6d5cc8b789902eb02c4fd5a3e36722492935c8e1ab224bccb8b753b062617
650a91ab990feed47adbd1f389674a8d718c25e3225a34a64f04ad82a497cb90147f4e54dbc513
cb0ac4d753cf7509e85df86e8298cf509000d5fbcdaecd3093b8a23a05261f0a2dafc0e1a89c8cb
17df3eba6306d1e76bc3f1eca27749b19a6969cebeaf714caccd393276aa49b2798baac6ef06346
d98434839aeda4fa926caa6f0e3e30180f28ead7049360728967f74face56a272a49070bd9489c
6a6e3a7836f93ea6ecb7978faade0a82e259a238a7e287c5a67d67b40f75682ae051cade6583f8d
ea06ba8c905b

66cd187775925a7c7f92e4499b0d14342d51fa246a4e43797fc431d9d3248fe234ec874eccc5a7
9871dd07e552aaf38779a1bd47ad6b555e716a722a38030614e43442ad0de7a47e17ceae19135
2a49706287ab3a36e754ff806c476d941d14e906ca373384ceb573904d0965b62d750d14c0638
3ef706b0768f49ed75359f0a1fb44fcb138c51763acf2c09006a04453217188f886346e8950376
9059bbe4d64b081dbda60f37a583dd6b7e83274098b799534a46c4e836cfa41946898998dc2b8
07dadc6db25d8c86145635afa7c12dbdf92ffc469bb5d49eb154253dab2d4b22653d90452bfea5
7c7005f0b610b5244e8e50fb385467bd7389ad22af1c2cb4007791b420dbde60fb675b748d433
60fdb5bdb3409f0c6d5cc8b789902eb02c4fd5a3e36722492935c8e1ab224bccb8b753b062617
650a91ab990feed47adbd1f389674a8d718c25e3225a34a64f04ad82a497cb90147f4e54dbc513
cb0ac4d753cf7509e85df86e8298cf509000d5fbcdaecd3093b8a23a05261f0a2dafc0e1a89c8cb
17df3eba6306d1e76bc3f1eca27749b19a6969cebeaf714caccd393276aa49b2798baac6ef06346
d98434839aeda4fa926caa6f0e3e30180f28ead7049360728967f74face56a272a49070bd9489c
6a6e3a7836f93ea6ecb7978faade0a82e259a238a7e287c5a67d67b40f75682ae051cade6583f8d
ea06ba8c905b

File Name :angel-search.json

1edc66e0448721e7801382cb0211625c730cf1450c642e271f3b6c30267aea2202022acd0a392
5071a2c18ba5d33a1e4f3abb8e753e438631b0c8fe4e325af31f68b726822419a72fd708d5ff312
7dd0cafc15a8a02b80278d258d874182b19b54f86fbf7eae0f1125c6be28aeff3e86bbf26570b49
b38f801f57fa916c210d01429451c764f42d97a3debb573e6be1d90c41936498651c023078101
4cd4c316f145efebd057eebd0fd331b1ecbc8367d2619f7a3d1db46af1a52630b806fd351061ff6
335b3a3a7d171eda48f13655db77633ecf15bb275df5e612ab865c2f9b4556105eaa22f2cc1914
7b84c13e9b88b84f8ccd873696b84d5627a5d9c6b802fead493266dd1f0dba489e9e314c43c19
d11aa909e270bd5eb9bbf3a7a63057bbf18bb3b08e44f2b3ec2318bac1301429c60bf3bcde7729
6afb97e2113457b5ceb5e47b91a94c095afbd4977ea30690ecedbfa68dc6b12ee181cddad3e5fb
0073fef5a328ab9d175e07ce64d356230dc4ede7598c77c5e63996a316544674c8fc1137547d0
310ee7055e69f77e83410a9636136f6e509e4d2231166c041591802ca3171619992057e545d99
08f1898cf20db45e8548c80a72348785be1fff5fac5661942d59c605f285c8bf8bdb407f29fbd7af
4679645287e3b99cc49f6ef5aea97e153d89b3c696d4937c2d475f34e3645acc331617af0554b4
d4a8ce774f

1edc66e0448721e7801382cb0211625c730cf1450c642e271f3b6c30267aea2202022acd0a392
5071a2c18ba5d33a1e4f3abb8e753e438631b0c8fe4e325af31f68b726822419a72fd708d5ff312
7dd0cafc15a8a02b80278d258d874182b19b54f86fbf7eae0f1125c6be28aeff3e86bbf26570b49
b38f801f57fa916c210d01429451c764f42d97a3debb573e6be1d90c41936498651c023078101
4cd4c316f145efebd057eebd0fd331b1ecbc8367d2619f7a3d1db46af1a52630b806fd351061ff6
335b3a3a7d171eda48f13655db77633ecf15bb275df5e612ab865c2f9b4556105eaa22f2cc1914
7b84c13e9b88b84f8ccd873696b84d5627a5d9c6b802fead493266dd1f0dba489e9e314c43c19
d11aa909e270bd5eb9bbf3a7a63057bbf18bb3b08e44f2b3ec2318bac1301429c60bf3bcde7729
6afb97e2113457b5ceb5e47b91a94c095afbd4977ea30690ecedbfa68dc6b12ee181cddad3e5fb
0073fef5a328ab9d175e07ce64d356230dc4ede7598c77c5e63996a316544674c8fc1137547d0
310ee7055e69f77e83410a9636136f6e509e4d2231166c041591802ca3171619992057e545d99
08f1898cf20db45e8548c80a72348785be1fff5fac5661942d59c605f285c8bf8bdb407f29fbd7af
4679645287e3b99cc49f6ef5aea97e153d89b3c696d4937c2d475f34e3645acc331617af0554b4
d4a8ce774f

File Name :angel-startups.json

dccae628aad26495c426781ac0071a5305a345063d0d032a67564432a3c2e73ff1c2722934444
d91494f6fa0a71882eab447c0fd8d0646d1f836b5811ca945c15bb6fc80f52ee5a2ce89d0e3866
167459bba49deb0b1073f37ea3d97e8db2a9b9111a7504037f6a9710e67e4bda95bc6a8d385e2
0404c0e3511e16297059032cee9184e35bffc3935ab7f852483043bbebc0e7166100e4722978a

b2fc858ff900915c335b484efe99596eea04a12318da97d834497a09f788ac0af001655d3578cfb
746ea29174e60af676b07b967b9c7b6c5066a8756368901035d91970c488bb7921f988d59652
81d196b09cbbd74a5219d4b0792abc241ebf3d6d048e9ae7e5727bea2d43044b547ec170c5d90
f441c9006be946fa49ff0d27836ecb1707947b89cb85a838aa1da7289f4ca41e3e0522d2e27ab3
2a58335fc0a7ccff750c2e700ba08d9d3e1506280fe9af7988240ec1aff0dba95e939a29704d908
4cd8152112abda9a623978f3894e3dd12bbcec436505dad6358c9aba72f06e4441152d3156e2ff
6a038a4b4d7bf9f95ac03dadef1adc215afbbad1f3925102c01fbc54c29721aa6c87b51f27723e6
d56de2db7cf0a49e1344dfadf9a19ad95bedfb517a1e5f1bc75acef152df27ab864c7ff979cca603
c7a5ee9de4e5cf2576b17a7ee3e188f8e7da538945889d527e3a1d294ac7417fdaf52bab270944
d347dc731d8
dccae628aad26495c426781ac0071a5305a345063d0d032a67564432a3c2e73ff1c2722934444
d91494f6fa0a71882eab447c0fd8d0646d1f836b5811ca945c15bb6fc80f52ee5a2ce89d0e3866
167459bba49deb0b1073f37ea3d97e8db2a9b9111a7504037f6a9710e67e4bda95bc6a8d385e2
0404c0e3511e16297059032cee9184e35bffc3935ab7f852483043bbebc0e7166100e4722978a
b2fc858ff900915c335b484efe99596eea04a12318da97d834497a09f788ac0af001655d3578cfb
746ea29174e60af676b07b967b9c7b6c5066a8756368901035d91970c488bb7921f988d59652
81d196b09cbbd74a5219d4b0792abc241ebf3d6d048e9ae7e5727bea2d43044b547ec170c5d90
f441c9006be946fa49ff0d27836ecb1707947b89cb85a838aa1da7289f4ca41e3e0522d2e27ab3
2a58335fc0a7ccff750c2e700ba08d9d3e1506280fe9af7988240ec1aff0dba95e939a29704d908
4cd8152112abda9a623978f3894e3dd12bbcec436505dad6358c9aba72f06e4441152d3156e2ff
6a038a4b4d7bf9f95ac03dadef1adc215afbbad1f3925102c01fbc54c29721aa6c87b51f27723e6
d56de2db7cf0a49e1344dfadf9a19ad95bedfb517a1e5f1bc75acef152df27ab864c7ff979cca603
c7a5ee9de4e5cf2576b17a7ee3e188f8e7da538945889d527e3a1d294ac7417fdaf52bab270944
d347dc731d8

Table 1, describes the integrity value of the proposed value to the traditional hash algorithms on different data types. From the table, it is noted that the present integrity model has better computational value than the traditional hash algorithms in terms of integrity runtime and bit change.

Table 2: Secret key generated using the encryption algorithm

E €Ž…oÜêø¼±Âú³-çÿCùy ~Ò½y•mþØ Ek7N, 3 # œ'ñETiì ØÝ£¢Œ{l'zà¼ÄêO7!çÉ,Å„ ½´&5¼{ ·©Ê~É›ä¡°¤ùÉ^BÙ¡,Hm=þ?b 'Ÿ<ú¯F\ i#Å¥Ô„Qõ^ ª°Ýúc[S €a6767874c74a5c9e591622a8a04445d4 853e3ecae93136faa4c4f0bcc422f1179	"®Û@®8 ±'›óé >ÿùF{·åÐ"Ýßv†œÃí|n0MÛêÈ¸à '°h·Â M=ðZ)S €83517460c323f8f0aa4c878976769096 94dea0dad0ca4a3fabb81dc1b362b1650 1b5757b8104970b667fea174f63a074dc

e41d049e2c5f276109407f5b86ee64f1f
5e9cc5aba4b1e9d884c3ef7e99e4ddE
€*æc™Tn*¢™‡ ÓQ«¨µŽ–ñJt åÞý:Ç<I-
…í\²

)j»eÈêÉàÆ~ËÞhàÂ¿ÎÙx½›ìêêQòâ¨ÚMÂ &
N³€AÑX2
¥>®Üÿ0n8I-À•O
———————————————xhïg~¬H‰ŠH¯
¶ÿëe¥^W¯°————————————————\æ
çñ\iyE
€ jEF(X¾]÷MœØ&£»Sùâ]µã2ï!ä]Ø¥Ž <
2`ãŠÛÂ²Ž8úÌoI¥AÀ-
?r =Ùd$3Ä\xEŽr2çS~Ùr¢ä*bÝÌRØ7c—
!Œáž3ÎÎŠ¼V +ë
î›KÔ˜Åð—hçzŽ\ËO Q¦ØŠR-PC¢ä‹sù S
€a9436f3c9eff7e0d8aab462822b50ed7
8f1619d8841c3ea5060d0fcf2bc83c20c
5cfd750e075118fccc1266ae945b49170
27280033233dba7bb13ebb948fd0a1E
€*æc™Tn*¢™‡ ÓQ«¨µŽ–ñJt åÞý:Ç<I-
…í\²

)j»eÈêÉàÆ~ËÞhàÂ¿ÎÙx½›ìêêQòâ¨ÚMÂ &
N³€AÑX2
¥>®Üÿ0n8I-À•O
———————————————xhïg~¬H‰ŠH¯
¶ÿëe¥^W¯°————————————————\æ
çñ\iyE
€ ïyó…°…}1‰YSÇà
———————————————LÈ%Œtýöã,Á'
É)$
÷(ðo2,¡9_·‰Ü¡]gè&®‟€ÙLùÂ·?Â&îô^w±
VÖgè

9ee29a6409614e4bbfec1b9a04a994E
€*æc™Tn*¢™‡ ÓQ«¨µŽ–ñJt åÞý:Ç<I-
…í\²

)j»eÈêÉàÆ~ËÞhàÂ¿ÎÙx½›ìêêQòâ¨ÚMÂ &
N³€AÑX2
¥>®Üÿ0n8I-À•O
———————————————xhïg~¬H‰ŠH¯
¶ÿëe¥^W¯°————————————————\æ
çñ\iyE €Eî¥ŸYŽ`¥ ñBŽy—
›£ÃùèkÃ¯~ìž˜bÈvÇÃÇáÍLx·Uð¦ý+¡Òê à
Nù€pvæÖ$½/ªýÛ Ce*‰%íÙÖÌUÅ|¸Úó^¶¤á
.cjÌ2òh)ÆàhU[c‟˜0ŠÀj;•=® ˆÜ~
Á¶µ¾S
€1c63c887e42912342dca20eed9624531
d7c1ad13fe790e57c377596ba2d7b2378
797f589e93c109498e9dd08d48d525653
10a5ca21ed4e3fe5843813c9c799e9E
€*æc™Tn*¢™‡ ÓQ«¨µŽ–ñJt åÞý:Ç<I-
…í\²

)j»eÈêÉàÆ~ËÞhàÂ¿ÎÙx½›ìêêQòâ¨ÚMÂ &
N³€AÑX2
¥>®Üÿ0n8I-À•O
———————————————xhïg~¬H‰ŠH¯
¶ÿëe¥^W¯°————————————————\æ
çñ\iyE €5ÓôÒPŠyJ‡qÂ¸š´H> ï
ŠèêÁuxŠjgæûÄq2øLkàzË Bwì<€)v›Hc5?
SZ&×™$ÿÔ-
}'²0õzƒÓªA[²˜ÚÍ|és® :¤

><#š‟˜© q'€

---

oFH)ª›1o]ûø~„¶ î½ @9S
€d439c95ae403bc8ec9df01e50b2ad2bf
b51c4b6840980121 93b32e31b286201fb
60dcf2893ac67892b9173b1520be74796
0fbd1e7481678a40a6c6b336cbb2acE
€*æc™Tn*¢™‡ ÓQ«¨µŽ–ñJt åÞý:Ç<I-
…í\²

)j»eÈêÉàÆ~ËÞhàÂ¿ÎÙx½›ìêêQòâ¨ÚMÂ &
N³€AÑX2
¥>®Üÿ0n8I-À•O
———————————————xhïg~¬H‰ŠH¯
¶ÿëe¥^W¯°————————————————\æ
çñ\iyE
€YS

¼3\Éý°8(‹™d‹ó+ÛØÆzOROÉ^< ýÚ_u³L
ýMÊÅ.µF&tÌöÅäª}Qbœïà>›ÖÍñ+t
)D D_*rÚ¯V9îüuJ V#U-
§É ß@‟`$¾Þ^é/ånÎu»ÝyÄg
———————————— †Ue„ÙÒÞ'JÑ
ä®

Table 2, describes the secret key value of the input data which is generated in the encryption process. This secret key is generated in the key generation phase of the proposed encryption model. This key is generated using the integrity value and the attributes list.

Table 3: MasterKey generation in the encryption process

E 5 Z Û Ç S ñ	‡<Ç.#Þ–¼ƒbÎEE € ¯šÁN¯Ä¹ 7ƒgÙýÌñõ5Î…– ”Y;@ µ«9Ub ‡kp®5 šÚx6m¨b x– Ü†%ù´úcTò.:$4‘sÈ+‡ß•¶\²¹’ ²Àv ^C e5üÿÂ¦4	Q	Š1Ù•‰@ˆá €‘%Ãý}`Ò ZgŸñÅÉ°è ž§ªE GA±]ßy«Ø ‹9x …´\Ï–á_E € €iÌCj8…Ù ôçßÎÄú} 1°¦˜ëz;ü ¥½xO™"– Øõ– Åˆ ÒÓNåU Š jÄw $k tP– OOŽ»–nþx Ýç `ûñŸ'“\ú õÚ'éI’¡« wäO’– ³C›÷ú3Œ‹ ÅP¤iXJ1ú åÿ4?!†/– <dI7Õ E {9–– †&iû/Z;Ü w$[;È¬Á E € X_†Vv6+g IN]ä<Ff½ Õ_~û? mÄ VVO#™¬¸ë QBuíÝNËà &¢Óà–ÒGE PøIéÓ›×« ìä›– Ô#Ó,Å#!< Nâ„)Ï·µ„ 0üà†lË”Ž F ÇäyDÿ'Ûm e™\ïŸKÜ_ ˜Gë¦	·hßþbv³„FÌ± ÛéIß˜KòÑûÂ˜™¤nÕ !¦KÜô¹þzE *}k N,Œ…‘<–ø·3ê7l¥w³E €~*–HZo9ÚD¥ÁÜMÙÛß _ì¿8& <eÛk×õ©þýbóÖN*žù Ð³ ƒGÐ‡PÝñ mÛ! R²âé Ð›r&žìÞL)àf¯ >°aú¥=µ‡:ª:ãE²0e)•± DP’ÂÇ…žWo!bz Òùp7A˜Š·‰ãy»QE }¾8ŽxH“€ìû>GãTwøE €'PÅSHëÁA[?ú"CXð¾´(ÒÀöÿ±u ‰&XJÙvX'p:¹¬Û;¤ùØêa ¥!°ï[t<ûKXì5öLYÈ‡ÿï'$5Ä?Õ•ô·{% ø2ÑjhÊR7¿:_É¹>y¢¨E¾"YŠïKD À|UÓÜ5˜e%€§Ï_)âê{]ÿÄE k ¡ œo¨ªAtì½€Ž æ X¢E €…1OQ'Œ5Ãüò ›%,ÉåK×Ï ôl~@ é‰Zõ/»§ ™B–øh#MšB[îé}Eš SÅ–”Áb@"¥ ™†ô°–AkÉüU²— 7Ùg|PòÏö¤«'úöyß$cÄ&& =¯Øå /*Yy0 ?1ïTuª– KÒÅžL1T™8µãÖE]s®·Ë+ +™yrÞðÔ·)Ò/E €1.%žö¯ ÒG ¬ÓRPyñé»a™”ô1‡ °„.“\O"î,‘Y†–ÀÕ— <~<voIZ˜ Ì¥& éFrrøœ8…œ¥Ð§£‰h& ËZÇS¦õ¸z šÚPèé,æ¶&€ |–,ï€È™!–PV `Õù\¥Ÿ¢ÞäT »E 0ž¥åüI™C‰÷‡R@‰E €:ç¨Z7®óT°2E;€ Z¹7¥aB6Hl0U'Q© ¾ÁãÇà}–Ç& ‘oJM°es Í}á£VR|µðYˆ«^¥L Š–8“2í¢l4ƒ°%éÉ:T– )vÃ,+?ˆd3únsI9q²¦InŒŒ ÃRu “w, é×™E 9çðŠxxkRVræRÕ4ûk¾E €˜Rp)µ,1%xR|ëÉàY½ã¡Í"OÍ¸° N`LÔVßü+!Â°†¦1ª:é”:ô^M]=Ž ßk˜ÅÎ /<Ý4|ë$FsG¡X6¿ VÓ_t ÌæÕ¯½n(^n÷ÒÍmoÑNMQšŒ.oç"Q > ¸~µw–ø ö”™ÂE	à ‡ I – / Þ

			UŸîÑÐ ¥B E >Asn«re' :®÷BÑëÄg îE €Uqâƒ'- 6UúJÈñ´o yÐf‹ `7ó] Ñï#=ŠJdG $Á£¬¤~eI ç÷Ô)à=‰˜ ÈØnS^©"z — Â©0Ÿ;epr W©K¡¹€}« (W›o Ã	pE\aGGWÜÐÌ,éýö×íÒô„mE €&›n×Ì¸ì”IIJÞü i3î,K#¨›Eb¡ öy,Xf-plŸ1ÆL·êø®S

Table 3, describes the master key value of the input data which is generated in the encryption process. This master key is generated in the setup phase of the proposed encryption model. This key is generated using the integrity value, policies list and the attributes list.

Table 4: Public Key:

E €- Òv÷žJ‹ÈÃ Æðv¹±Žûáôûo- Î®òa,>Ø‡çnãS Ä»I5Š‹^DcLÆú Y‰LÕ p÷$wOkí ¼.3YP¶=‰ñõM˜ ²={Íá1±7ªä°: ç]":EÈÔ±[…„	É î,Ý^ôQ[=ôõ5š ¨(t!ÄŒíý‹&ôà ›wŒèLïõåœ^ìZ ±¾0®þãúÏ%ùîD "yôÍ^îÌ·êƒ	ˆ Ý Û Q à V E € O ” : â - µ » N ø š ï 9 þ ª å n …	Q Ó ° # O ¥ 8 & £ ß ” $ ½ à ê 7 é] ° ù Î ù ê î µ ! « + Q y	Œ ¢ ; † o Á 4 x Y Á g b µ Ø û £	¢ °M+RàãOñÆ\á„ ˜ ž®„›ì`}ö`rÜè ÄÃsFÍ[öÝ%¸˜š Âa1ƒÄÔ™m¡àÄ %qG= ÿÑ:ðÞÃÄ ÓÙ'ÈÀSÛ^~tÎR	E € v / í Å " ˆ ¯ ª	Ï õ\ Î¢ cç Ü‹ Ù6 'À ‹• ûR F5 ã° ÊT ˜- (à …Ç ‰= Ê§ ˆù jE 7ß p_ , ØH ¹3 ê‹ ¸á >† ¶Ð à fm ‹t	Œ]tÂŠA>8Ä‡Ï ÍÀÏ'†QD$ÀöOs ý¡c838D²°&¨ì ÞëE € :žT…ÿÒ &Áj›f\Î- Ú¸àb·qfø¯÷j5 ùCv¬ »'6 à¨ EBàHd<ÈóÀhÛ¿ Ýd˜ Ã$-‡PLì; +L ² 4õ‹ö*gA O E¬žò— ÿUaz±îÞë¦?`† ±<ƒÚ)¡fŽ ›®i—MeU]ÎŸE €— R "´ò°ž ÏéÔàÍë0¦5V- Å{†ñ¤ÏB ?`Í0Ö('¿ú"ÛÄ ½Ê5os˜}lx2‡-
%jE €šõ'¤A+?Oô" M2 "b¬… O								

		„µŒb¨ Œ–ù= 2†ƒôr É#¦¾` Æ åI	«– ¦ãã[z°\u¦¦ ÷³*ßx\· —÷æ$j·jBº —Ÿ€BëévÿžžŸ ØÐ2E€/qIJ%äîòÖà …ÚÌÓ				öv âÜŽõ A¹	

			$ › æ Å ¥ ?					

Table 4, describes the public key value of the input data which is generated in the encryption process. This public key is generated in the setup phase of the proposed encryption model. This key is generated using the integrity value, policies list and the attributes list.

Table 5: Sample Encrypted Data for the e-governance data

```
PI____S_€a6767874c74a5c9e591622a8a04445d4853e3ecae93136faa4c4f0bcc42
2f1179e41d049e2c5f276109407f5b86ee64f1f5e9cc5aba4b1e9d884c3ef7e99e4d
dE___€ŒÈ__£G_cÙÕ`¨Ä†Ïá"Gú_ù—
®ÒÔ rý_üè_s_ŒIB2_C†±§ ìüÑzÛ hš>P0€à‰A¹p& _UÌ_¡¸s˜£²¿aõ OíÅD1 _-
íBËù_û'_<Ø”ø,™
]tJ_¶”À7yß¦dq/ß¸ PXKœ_zð_{¡E___€a6767874c74a5c9e591622a8a04445d4853e
3ecae93136faa4c4f0bcc422f1179e41d049e2c5f276109407f5b86ee64f1f5e9cc5
aba4b1e9d884c3ef7e99e4dd[____E___€‰_:â]Özúã†e•b”ƒ½'G*¹Ù#„÷_u__Í¢„ @
_ð7‰°\Üh›bk|{E_ì>ÈþF-E, -_eÕ•cßóøü{JvÈÂ¶_¬_ð9r_y’-
°êÄ§ó(ä:ÿg_ôÍ>ÝYm¶JE õƒ&U:^#¨¹Å0-
¶Tþ>°,Ãi:ÁE___€_H_Š_Oä8 ì7_^¢34o ò£_-¡N•é_ßÚi¥O;ßuK± , ×¹I_$#…#f
      ö‰A_Måê›_Ê}N¥Q¤_Ã¨Ç+,Ÿÿ«!z©Úôg …1^>¯2ÖÙËôÖ—ý_ƒ_rU¾ [_Ò_h!E°¾-
þ5méw1ëÞ3ë<Õ¡¾t0~:ÖÚ£_òóÀaÙzìë,^
³Zký †1ø_ z˜h“8°æ_&j¬|›ø„žh`¼¶úå j=øØ “þ_Þ
oR<_p+CAÍV2jT/l»_Ä^+Jì4ýýýl„ <g[_°~_`ïD… Mï_,â
      7øÐx”_p«_÷Ä $_ußT_=å
```

Table 5, represents the encrypted cipher text value of the input e-governance dataset. As shown in the table 5, as the size of the input data increases, proposed model less storage cipher text value in the cloud environment.

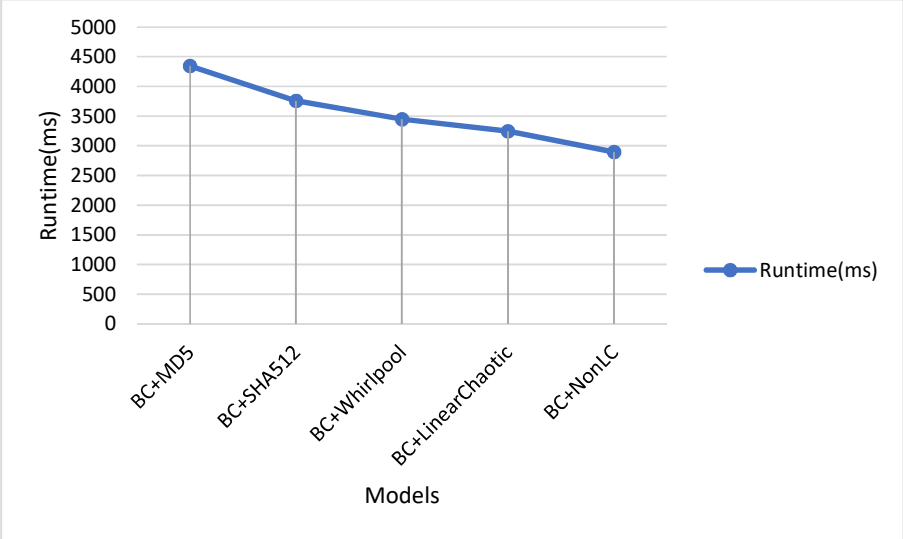

Figure 3: Comparative analysis of proposed model to existing models in terms of hash runtime(ms)

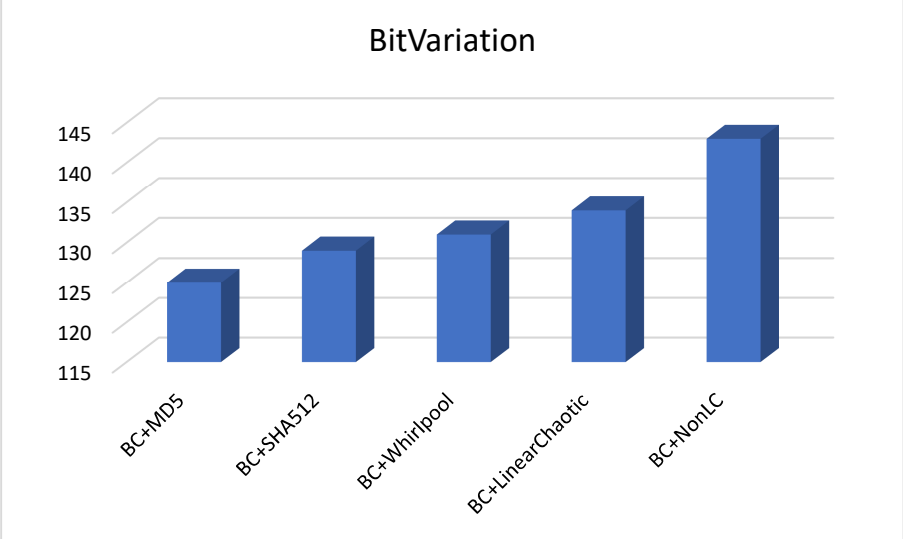

Figure 4: Comparative analysis of proposed model to existing models in terms of hash bitchange variation.

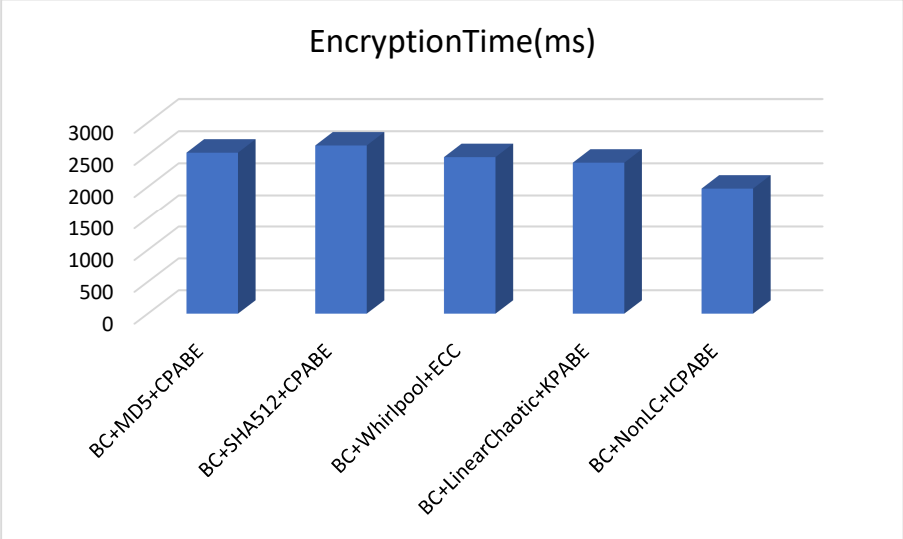

Figure 5: Comparative analysis of proposed model to existing hash based encryption models in terms of runtime(ms)

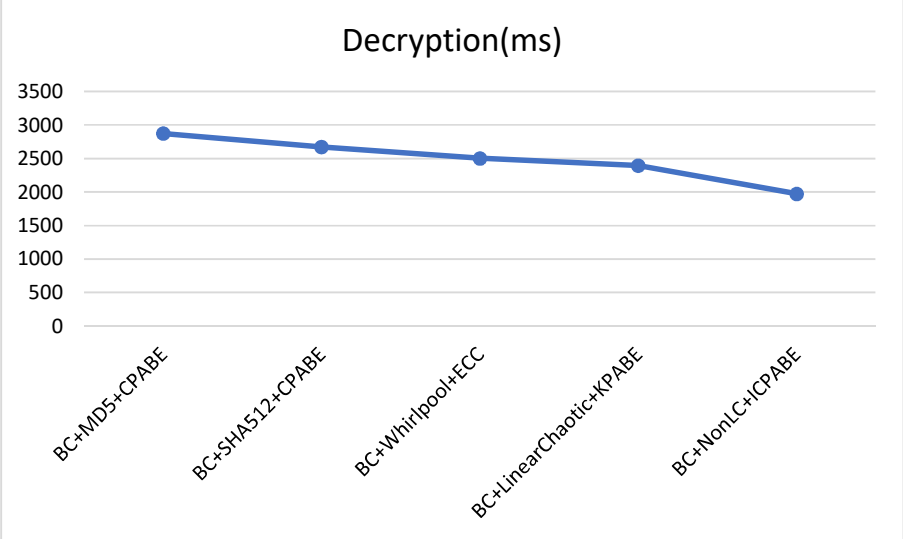

Figure 6: Comparative analysis of proposed model to existing hash based decrption models in terms of runtime(ms).

Conclusion

In this paper, a hybrid block-chain framework is implemented on the large media files. This framework is tested on the both the private and public cloud servers. Most of the conventional block-chain frameworks are based on the existing integrity and confidentiality models. Also, these models are based on the data size and file format. In order to overcome these problems in the cloud computing environment, a hybrid integrity and security-based block-chain framework is designed

and implemented on the large media data types. In this framework, a novel non-linear chaotic function-based hash algorithm and advanced attribute-based encryption models are used to improve the traditional block chain framework on the large cloud datasets. Experimental results proved that the proposed advanced block-chain technology has nearly 7% improvement than the traditional security models in terms of hash bit variation, hash runtime(ms), encryption and decryption time.

References

[1]N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "An efficient attribute-based online/offline searchable encryption and its application in cloud-based reliable smart grid," Journal of Systems Architecture, vol. 98, pp. 165–172, Sep. 2019, doi: 10.1016/j.sysarc.2019.07.005.

[2]A. S. Voundi Koe and Y. Lin, "Offline privacy preserving proxy re-encryption in mobile cloud computing," Pervasive and Mobile Computing, vol. 59, p. 101081, Oct. 2019, doi: 10.1016/j.pmcj.2019.101081.

[3]G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Computers & Security, vol. 30, no. 5, pp. 320–331, Jul. 2011, doi: 10.1016/j.cose.2011.05.006.

[4]H. Wang, Y. Zhang, K. Chen, G. Sui, Y. Zhao, and X. Huang, "Functional broadcast encryption with applications to data sharing for cloud storage," Information Sciences, vol. 502, pp. 109–124, Oct. 2019, doi: 10.1016/j.ins.2019.06.028.

[5]G. Wei, R. Lu, and J. Shao, "EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption," Journal of Computer and System Sciences, vol. 80, no. 8, pp. 1549–1562, Dec. 2014, doi: 10.1016/j.jcss.2014.04.021.

[6]Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K.-K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," Pervasive and Mobile Computing, vol. 28, pp. 122–134, Jun. 2016, doi: 10.1016/j.pmcj.2015.06.017.

[7]M. Zhao E and Y. Geng, "Homomorphic Encryption Technology for Cloud Computing," Procedia Computer Science, vol. 154, pp. 73–83, Jan. 2019, doi: 10.1016/j.procs.2019.06.012.

[8]X. Zheng, Y. Zhou, Y. Ye, and F. Li, "A cloud data deduplication scheme based on certificateless proxy re-encryption," Journal of Systems Architecture, vol. 102, p. 101666, Jan. 2020, doi: 10.1016/j.sysarc.2019.101666.

[9]I.-C. Lin, C.-Y. Cheng, and H.-Y. Chen, "A real-time parking service with proxy re-encryption in vehicular cloud computing," Engineering Applications of Artificial Intelligence, vol. 85, pp. 208–213, Oct. 2019, doi: 10.1016/j.engappai.2019.05.013.

[10]M. Rady, T. Abdelkader, and R. Ismail, "Integrity and Confidentiality in Cloud Outsourced Data," Ain Shams Engineering Journal, vol. 10, no. 2, pp. 275–285, Jun. 2019, doi: 10.1016/j.asej.2019.03.002.

[11]P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, “Blockchain data-based cloud data integrity protection mechanism,” Future Generation Computer Systems, vol. 102, pp. 902–911, Jan. 2020, doi: 10.1016/j.future.2019.09.028.

[12]S. Singh and S. Thokchom, “Public integrity auditing for shared dynamic cloud data,” Procedia Computer Science, vol. 125, pp. 698–708, Jan. 2018, doi: 10.1016/j.procs.2017.12.090.

[13]Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong, and J. Lei, “One secure data integrity verification scheme for cloud storage,” Future Generation Computer Systems, vol. 96, pp. 376–385, Jul. 2019, doi: 10.1016/j.future.2019.01.054.

[14]L. Ferretti, M. Marchetti, M. Andreolini, and M. Colajanni, “A symmetric cryptographic scheme for data integrity verification in cloud databases,” Information Sciences, vol. 422, pp. 497–515, Jan. 2018, doi: 10.1016/j.ins.2017.09.033.

[15]Q. Wu, F. Zhou, J. Xu, and Q. Wang, “Secure data stream outsourcing with publicly verifiable integrity in cloud storage,” Journal of Information Security and Applications, vol. 49, p. 102392, Dec. 2019, doi: 10.1016/j.jisa.2019.102392.

[16]Y. Yan, L. Wu, G. Gao, H. Wang, and W. Xu, “A dynamic integrity verification scheme of cloud storage data based on lattice and Bloom filter,” Journal of Information Security and Applications, vol. 39, pp. 10–18, Apr. 2018, doi: 10.1016/j.jisa.2018.01.004.

[17]L. Zhou, A. Fu, S. Yu, M. Su, and B. Kuang, “Data integrity verification of the outsourced big data in the cloud environment: A survey,” Journal of Network and Computer Applications, vol. 122, pp. 1–15, Nov. 2018, doi: 10.1016/j.jnca.2018.08.003.

[18]N. Garg and S. Bawa, “Comparative analysis of cloud data integrity auditing protocols,” Journal of Network and Computer Applications, vol. 66, pp. 17–32, May 2016, doi: 10.1016/j.jnca.2016.03.010.

[19]M. M. Al-Sayed, H. A. Hassan, and F. A. Omara, “CloudFNF: An ontology structure for functional and non-functional features of cloud services,” Journal of Parallel and Distributed Computing, vol. 141, pp. 143–173, Jul. 2020, doi: 10.1016/j.jpdc.2020.03.019.

[20]J. Guo et al., “A geometry- and texture-based automatic discontinuity trace extraction method for rock mass point cloud,” International Journal of Rock Mechanics and Mining Sciences, vol. 124, p. 104132, Dec. 2019, doi: 10.1016/j.ijrmms.2019.104132.

[21]J. Li, “Resource optimization scheduling and allocation for hierarchical distributed cloud service system in smart city,” Future Generation Computer Systems, vol. 107, pp. 247–256, Jun. 2020, doi: 10.1016/j.future.2019.12.040.

[22]A. Nadjaran Toosi, J. Son, Q. Chi, and R. Buyya, “ElasticSFC: Auto-scaling techniques for elastic service function chaining in network functions virtualization-based clouds,” Journal of Systems and Software, vol. 152, pp. 108–119, Jun. 2019, doi: 10.1016/j.jss.2019.02.052.

[23]P. Sharma, D. Arora, and T. Sakthivel, “Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications,” Procedia Computer Science, vol. 167, pp. 907–917, Jan. 2020, doi: 10.1016/j.procs.2020.03.390.

[24]H. Wang, H. Qin, M. Zhao, X. Wei, H. Shen, and W. Susilo, “Blockchain-based fair payment smart contract for public cloud storage auditing,” Information Sciences, vol. 519, pp. 348–362, May 2020, doi: 10.1016/j.ins.2020.01.051.

[25]S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, “Blockchain for cloud exchange: A survey,” Computers & Electrical Engineering, vol. 81, p. 106526, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106526.

[26]Z. Zhu, G. Qi, M. Zheng, J. Sun, and Y. Chai, “Blockchain based consensus checking in decentralized cloud storage,” Simulation Modelling Practice and Theory, p. 101987, Sep. 2019, doi: 10.1016/j.simpat.2019.101987.

[27]S. Alansari, F. Paci, A. Margheri, and V. Sassone, “Privacy-Preserving Access Control in Cloud Federations,” in 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Jun. 2017, pp. 757–760, doi: 10.1109/CLOUD.2017.108.

[28]E. Bellini, P. Ceravolo, and E. Damiani, “Blockchain-Based E-Vote-as-a-Service,” in 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), Jul. 2019, pp. 484–486, doi: 10.1109/CLOUD.2019.00085.

[29]H. Qiu, X. Wu, S. Zhang, V. C. M. Leung, and W. Cai, “ChainIDE: A Cloud-Based Integrated Development Environment for Cross-Blockchain Smart Contracts,” in 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Dec. 2019, pp. 317–319, doi: 10.1109/CloudCom.2019.00055.