**1**

**CLOUD COMPUTING**

**IEEE, 2019 (Conference Paper)**

**a28**

@inproceedings{kumar2019review,

title={A review on hybrid encryption in cloud computing},

author={Kumar, Lalit and Badal, Neelendra},

booktitle={2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)},

pages={1--6},

year={2019},

organization={IEEE}

}

**Abstract** - In today world scenario, user wants to keep our

data in storage as well as on cloud, so in cloud user uses

cloud storage. To provide security to cloud storage user

uses hybrid encryption instead of single encryption

algorithm. In this paper user provides some previous

information about that types of works and the major focus

the user is on the hybrid approach of **AES and FHE.** This

hybrid approach helps the user to keep data into more

redundant and secure in comparisons of some others. By

using this method, user can protect data confidentiality,

privacy and integrity from the hackers. In this

methodology section of this paper user also discuss about

its working by using flowchart and algorithm to

understand this approach properly.

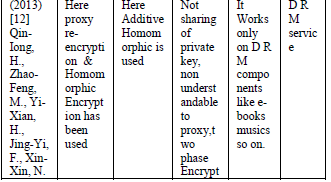
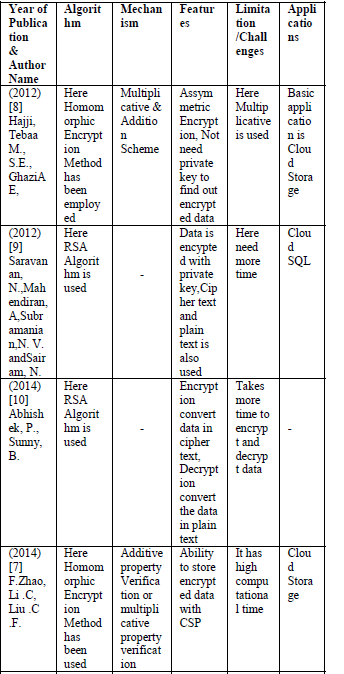
**Contribution-**

* This has given a protected entry of information over the Internet, the dependable key age process, double encryption processes lastly check of clients.
* The proposed work has got explicit highlights by decoding in absentia private key and in

fast.

**Limitation-**

The future work will be the work making this work perfect with all cloud administrations which move toward becoming as a confinement in this work.



**2.Data Access Security in Cloud Computing: A**

**Review**

**IEEE,2018**

**a1**

@INPROCEEDINGS{8675033, author={Markandey, Anagha and Dhamdhere, Prajakta and Gajmal, Yogesh}, booktitle={2018 International Conference on Computing, Power and Communication Technologies (GUCON)}, title={Data Access Security in Cloud Computing: A Review}, year={2018}, volume={}, number={}, pages={633-636}, doi={10.1109/GUCON.2018.8675033}}

**Abstract-**Nowadays, big data is stored on the internet called clouds. With usage of cloud storage users can store their data on the internet. Cloud computing provides

various services to the users. Data storage is one of them. But it is observed that there is a very big problem of data stealing through the internet. More is the problem of data leaking &

attacks on the data on clouds. The intention of this paper is **to attain data security of cloud storage and to put together an equivalent cloud storage security strategy**. These strategies are

combined with the outcomes of existing data by considering the security risks & user data on cloud storage & move towards the appropriate security technique , which is based on

properties of cloud storage systems. The paper will go in to subtle elements of information assurance strategies and methodologies utilised all through the world to guarantee most

extreme information insurance by diminishing dangers and dangers. Accessibility of information in the cloud is helpful for some applications yet it postures hazards by presenting

information to applications which may as of now have security provisos in them. Also, utilisation of virtualization for distributed computing may change information when a visitor OS is kept running over a hypervisor without knowing the unwavering quality of the visitor OS which may have a security provision in it. The paper will likewise give a knowledge on information security perspectives for Data-in-Transit and Data-at-Rest.

**Contribution-**In this paper authors presented a model for provable the

information ownership (PDP) that permits a customer that

has put away information at an untrusted server to confirm

that the server has the first information without recovering it.

The model creates probabilistic verifications of ownership

by inspecting arbitrary arrangements of squares from the

server, which definitely decreases I/O costs.

**Limitation- Future scope-** Data Classification in view of Security,Character administration framework,Secure put stock in based Solution for distributed computing Service.

**3.Enhancing Security of Health Information Using**

**Modular Encryption Standard in**

**Mobile Cloud Computing**

**IEEE Access,2021**

**a24**

**@article{shabbir2021enhancing,**

**title={Enhancing security of health information using modular encryption standard in mobile cloud computing},**

**author={Shabbir, Maryam and Shabbir, Ayesha and Iwendi, Celestine and Javed, Abdul Rehman and Rizwan, Muhammad and Herencsar, Norbert and Lin, Jerry Chun-Wei},**

**journal={IEEE Access},**

**volume={9},**

**pages={8820--8834},**

**year={2021},**

**publisher={IEEE}**

**}**

**Abstract-**Despite the numerous and noticeable inherited gains of Mobile Cloud Computing (MCC) in

healthcare, its growth is being hindered by privacy and security challenges. Such issues require the utmost urgent attention to realize its full scale and efcient usage. There is a need to secure Health Information worldwide, regionally, and locally. To fully avail of the health services, it is crucial to put in place the demanded security practices for the prevention of security breaches and vulnerabilities. Hence, **this research is deliberated on to provide requirement-oriented health information security using the Modular Encryption Standard (MES) based on the** layered modeling of the security measures. The performance analysis shows that the proposed work excels, compared to other commonly used algorithms against the health information security at the MCC environment in terms of better performance and auxiliary qualitative security ensuring measures.

**Contribution-**

The proposed work provides secure HI storage against

ensuring the condentiality of the cloud service

Provider.

It ensures the condentiality of HI against any hacker or

third party/malicious outsider.

It provides a requirement centric approach against ensuring

the condentiality of HI (i.e., separate classication

of security provision based on the sensitivity level of HI).

Full control of the patient to their HI.

Unwanted attempt to access the HI would be restricted.

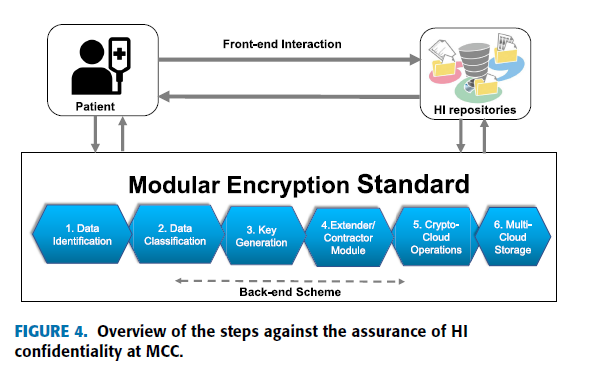
Only the patient has full access to his data. Also, based

on a requirement can be shared with others i.e., specialists

and experts.

Layered modeling with modularity support against the

intruder's attacks to HI.

****

**Limitation-** this approach is intended for the enciphering and deciphering of textual data and there is **no consideration of the image-oriented data-set** yet.

Layered modelling may sometimes result in **lowering system efficiency**. Accordingly,

The efficiency of the proposed work can be further improved by the integration of quantum computing to make it more adaptable for mobile and smart devices.

**4.Assessing information security risks in the cloud: A case study of Australian**

**local government authorities**

**Elsevier,2019(Journal)**

**@article{ali2020assessing,**

**title={Assessing information security risks in the cloud: A case study of Australian local government authorities},**

**author={Ali, Omar and Shrestha, Anup and Chatfield, Akemi and Murray, Peter},**

**journal={Government Information Quarterly},**

**volume={37},**

**number={1},**

**pages={101419},**

**year={2020},**

**publisher={Elsevier}**

**}**

**a11**

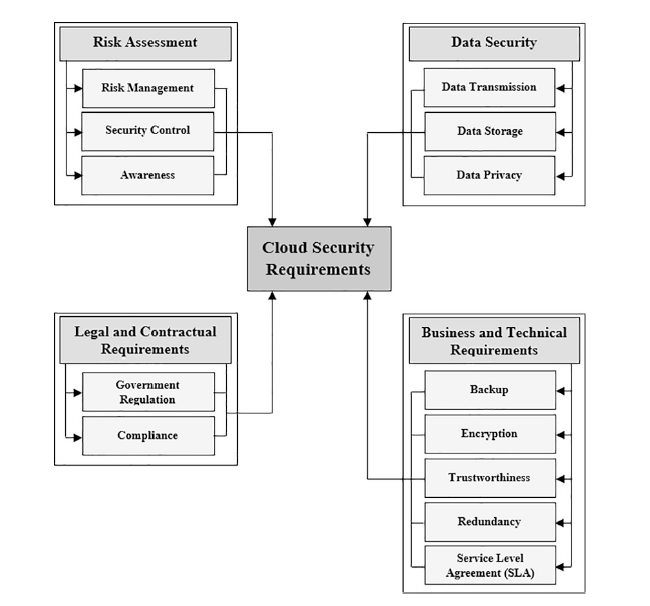
**Abstract-**Cloud computing enables cost-effective and scalable growth of IT services that can enhance government services.

Despite the Australian Federal Government's ‘cloud-first’ strategy and policies, and the Queensland State Government's ‘digital-first’ strategy, cloud services adoption at local government level has been limited—largely due to data security concerns. We reviewed the ISO 27002 Information Security standard with extant literature and found that operational security, individual awareness and compliance matters pose more significant government challenges than the often-highlighted technical and process-oriented cloud security requirements. This study identifies and explores the critical factors associated with information security requirements of cloud services within the Australian regional local government context. We conducted 21 field interviews with IT

managers, and surveyed 480 IT staff from Australia's 47 regional local governments. We propose a conceptual

cloud computing security requirements model with four components – data security; risk assessment; legal & compliance requirements; and business & technical requirements – in order to promote a balanced view on cloud security for governments. Using this model, governments can work together to demand uniform security requirements for adopting cloud services.

**Contribution-**

****

This research expands scholarly knowledge about the critical factors

related to the security requirements for cloud computing in regional

local governments. We found that technology and process maturity for

cloud security requirements is high; however, operational maturity,

people awareness and legal environments provide significant challenges

that must be addressed in future research and practice.

**5.INFORMATION SECURITY IN CLOUD COMPUTING**

**ijitcs,2013**

**Abstract-**In cloud computing IT (Information Technology) related resources like infrastructure, platform and software can be utilized using web based tools and application through internet. Here Organizations are moving to the cloud computing some faster than others. However, moving to the cloud presents the organization with a number of risks to assess. Information security is the most critical risk for many organizations. This is because the intellectual property, trade secrets, personally identifiable information, or other sensitive information can be powered by protecting information. This paper classified cloud security based on the three service models of cloud computing SaaS, PaaS and IaaS. Attributes for each type of security has also identified and briefly described here. **We compared securities provided in different services by world's best known cloud service providing companies such as Amazon AWS, Google App Engine, Windows Azure etc. considering cloud security category**. Furthermore, we included recommendations for organizations who have decided to move their data into the cloud, but confused to choose the best service provider for their organization regarding information security.

**6.A Systematic Review of the Security in Cloud**

**Computing: Data Integrity, Confidentiality and**

**Availability**

**IEEE,2020**

**a2**

**@INPROCEEDINGS{9231255, author={Kumar, Rajeev and Bhatia, M P S}, booktitle={2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)}, title={A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability}, year={2020}, volume={}, number={}, pages={334-337}, doi={10.1109/GUCON48875.2020.9231255}}**

**Abstract-**The cloud computing plays the prominent role in

many organizations and researchers were focus on securing the

cloud computing. The privacy preserving is the major

challenge that grows exponentially with increases in user. In

this paper, the depth survey is conducted on the recent

methodologies of the cloud storage security related with the

cloud computing. The overview of the cloud computing and

security issues is analyzed in this paper. The key security

requirements such as data integrity, availability and

confidentiality. Security issues in the recent methodologies of

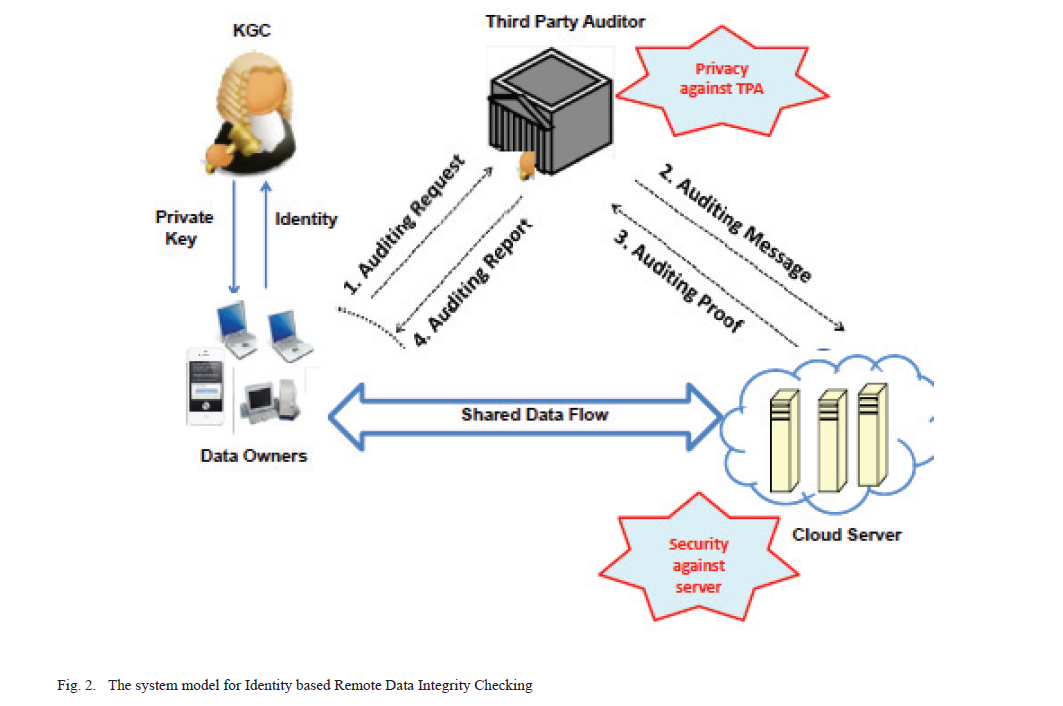
cloud security is analyzed. The challenges in the cloud security

is analyzed and possible future scope of the method is

discussed. The paper involves in **analyzing the state-of-art**

**method to investigate the advantages and limitations.**

**Contribution-**

****

Challenges..

**7.Privacy Protection and Data Security in**

**Cloud Computing：A Survey, Challenges**

**and Solutions**

**IEEE,2019**

**a12**

**@article{sun2019privacy,**

**title={Privacy protection and data security in cloud computing: a survey, challenges, and solutions},**

**author={Sun, Pan Jun},**

**journal={IEEE Access},**

**volume={7},**

**pages={147420--147452},**

**year={2019},**

**publisher={IEEE}**

**}**

**Abstract-**Privacy and security are the most important issues to the popularity of cloud computing

service. In recent years, there are many research schemes of cloud computing privacy protection based on access control, attribute-based encryption (ABE), trust and reputation, but they are scattered and lack unified logic. In this paper, we systematically review and analyze relevant research achievements. First, we discuss the architecture, concepts and several shortcomings of cloud computing, and propose a **framework of privacy protectio**n; second, we discuss and **analyze basic ABE, KP-ABE (key policy attribute-based encryption), CP-ABE (ciphertext policy attribute-based encryption), access structure, revocation mechanism, multi-authority, fine-grained, trace mechanism, proxy re-encryption(PRE), hierarchical encryption, searchable encryption(SE), trust, reputation, extension of tradition access control and hierarchical key**; third, we propose the research challenge and future direction of the privacy protection in the cloud computing; finally, we point out corresponding **privacy protection laws** to make up for the technical deficiencies.

**Testing and Evaluation System for Cloud Computing Information**

**Security Products**

**elseviar,2019**

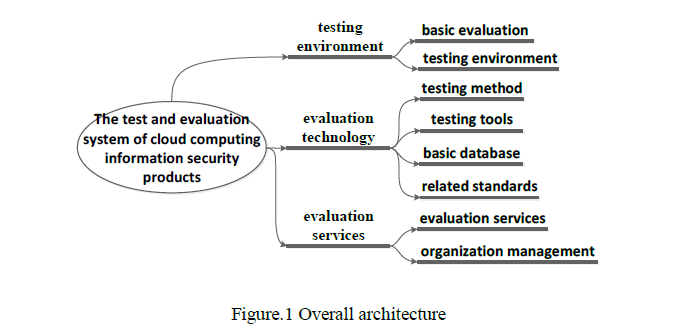
**Abstract-**Due to the lack of professional testing and evaluation system for cloud computing information security products, the basic

security of cloud computing information security products cannot be guaranteed. The establishment of a test and evaluation

system of cloud computing information security products is provided, and the system is used in the actual product testing, to

further promote the development of cloud computing and information security

**Contribution-**

****

**8.Secure and Efficient Image Retrieval over Encrypted Cloud Data**

**A18**

**Hindawi,2018**

**@article{liang2018secure,**

**title={Secure and efficient image retrieval over encrypted cloud data},**

**author={Liang, Haihua and Zhang, Xinpeng and Cheng, Hang and Wei, Qiuhan},**

**journal={Security and Communication Networks},**

**volume={2018},**

**year={2018},**

**publisher={Hindawi}**

**}**

**Abstract-**This paper proposes a novel image retrieval scheme over encrypted cloud data, which achieves high efficiency and confidentiality.

For the purpose of improving search efficiency, an index tree is often deployed in the image retrieval scheme. Meanwhile, the confidentiality of the sensitive cloud data, such as outsourced images, index tree, and query request, is also a key issue. Firstly**, a balanced binary clustering algorithm is exploited over the integrated image features composed of basic features, such as HSV**

**histogram and DCT histogram, yielding a balanced binary tree (BBT**). In particular, due to the adoption of a balanced index tree, our scheme can achieve logarithmic search time. Secondly, the secure inner product is employed to encrypt the index vector and query feature. Finally, to resist the statistical attack of the frequency distribution of the retrieved results, we copy the database and

merge the subtree of encrypted BBT to blind the search results. Security analysis and experimental results show that the proposed scheme is secure and efficient.

**Contribution-**

(1) We combine HSV histogram in the color space and

DCT histogram in the transform domain as an integrated

feature. To improve the search efficiency, we construct a BBT

for the image database. The BBT is built from a top-down

approach. Since the hierarchical index tree is approximately

balanced, the scheme can achieve logarithmic search time.

(2) By incorporating secure inner product (i.e., ASPE),

the BBT is encrypted as secure BBT (SBBT) by a secret

key, and query feature is encrypted. The database image is

encrypted by another secret key. After that, the sensitive

data in the cloud is protected; meanwhile, the searchable

functionality of the encrypted feature is still valid. Further,

the random number extended in the query feature can blind

the query pattern.

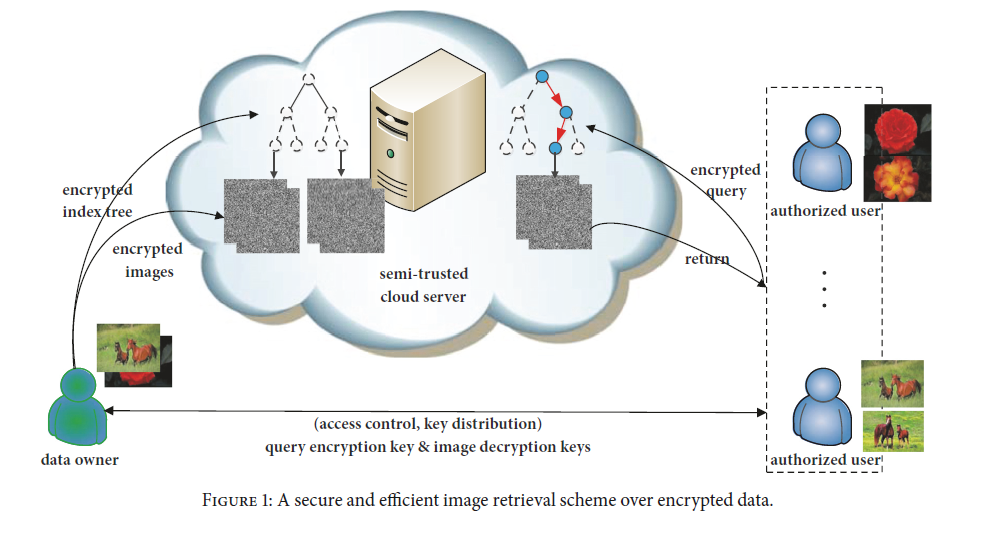
(3) To blind the search result, we copy the database and

merge the subtree to rebuild SBBT. The reduced SBBT and

the weighted factor of the integrated feature make the search

result of one query image not unique. Therefore, the query

privacy about access pattern is protected



**Limitation-**In future, we will improve the ASPE to support multi user scenario, where a dishonest user may try to reveal the encrypted query of other users. It is also a meaningful work to generate a generic, high-semantic feature.

**9.Attribute-Based Encryption from Identity-Based**

**Encryption**

* **2017 ,Computer Science, Mathematics**

**a19**

**@article{Fan2017AttributeBasedEF,**

**title={Attribute-Based Encryption from Identity-Based Encryption},**

**author={Chun-I Fan and Yi-Fan Tseng and Chih-Wen Lin},**

**journal={IACR Cryptol. ePrint Arch.},**

**year={2017},**

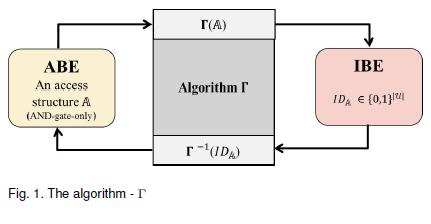
**volume={2017},**

**pages={219}**

**}**

**Abstract-**Ciphertext-policy attribute-based encryption (CP-ABE) is an access control mechanism where a data provider encrypts a secret message and then sends the ciphertext to the receivers according to the access policy which she/he decides. If the attributes of the receivers match the access policy, then they can decrypt the ciphertext. This manuscript shows a relation between ABE and identity-based encryption (IBE), and presents a bi-directional conversion between an access structure and identities. By the proposed conversion, the ABE scheme constructed from an IBE scheme will inherit the features, such as constant-size ciphertexts and anonymity, from the IBE scheme, and vice versa. It turns out that the proposed conversion also gives the first ABE achieving access structures with wildcard and constant-size ciphertexts/private keys.

**Contribution-**

****

****

**Limitation-**In the future, we will provide the proofs for the uniqueness

of the proposed conversion methods and the CCA security

proofs for confidentiality and anonymity to demonstrate the

security of the proposed conversion methods.

**10.A Comparative Study of Applying Real-Time**

**Encryption in Cloud Computing Environments**

**IEEE,2013**

**a4**

**@INPROCEEDINGS{6710575, author={Fatemi Moghaddam, Faraz and Karimi, Omidreza and Alrashdan, Maen T.}, booktitle={2013 IEEE 2nd International Conference on Cloud Networking (CloudNet)}, title={A comparative study of applying real-time encryption in cloud computing environments}, year={2013}, volume={}, number={}, pages={185-189}, doi={10.1109/CloudNet.2013.6710575}}**

**Abstract-**The rapid growth of cloud computing as a

newfound technology and many unclear security issues in it cause

many challenges. These challenges are specified in service

provider’s cloud servers and transmission processes.

Accordingly, this paper presents a model based on separate data

and key cloud servers and a client-based data encryption service

for increasing the reliability in cloud computing environments. In

the proposed model, the key generation process is done in a

separate cloud application and public and private keys are stored

in key cloud servers. Moreover, the encryption and decryption

processes are done in client side by a service that named “data

encryption service”. For applying this encryption system a

comparative study was done by **analyzing the strengths and**

**weaknesses of six popular asymmetric key encryption algorithms**

**(i.e. Original RSA, RSA Small-e, RSA Small-d, MREA, E-RSA,**

**and EAMRSA) according to time, key size and security**

**parameters.** These algorithms were briefly described and

redeveloped in the same situation for the simulation process to

investigate the performance in client-based data encryption

service. Furthermore, the security analysis was done by

reviewing the performance of described algorithms against three

popular attacks: Brute Force, Mathematical, and Timing Attack.

According to the results E-RSA in the most appropriate

algorithm for using in client-based data encryption service by

achieving acceleration, accuracy, and security in this service

based on compatibility issues in a client side service.

**Contribution-**

RSA Small-e and E-RSA algorithms are more efficient in large size files.

Total execution time in RSA Small-e is less than other algorithms according to the small size of public exponent.

Time for encryption and decryption, RSA Small-e and E-RSA seems to be more logical in comparison with other in nature of data encryption service.

**11.An Introduction to Identity-based Cryptography,2005**

****

Biometric based

**12.Automated Biometric Authentication with Cloud Computing**

**Springer,2019**

**a13**

**@incollection{al2019automated,**

**title={Automated biometric authentication with cloud computing},**

**author={Al-Assam, Hisham and Hassan, Waleed and Zeadally, Sherali},**

**booktitle={Biometric-based physical and cybersecurity systems},**

**pages={455--475},**

**year={2019},**

**publisher={Springer}**

**}**

**Abstract-**Over the last few years, cloud computing has become one of the fastest-growing IT

environments for providing services to individuals and businesses of all sizes. Cloud

computing, as defined by the National Institute of Standards and Technology

(NIST), is “a model for enabling ubiquitous, convenient, on-demand network access

to a shared pool of configurable computing resources (e.g., networks, servers,

storage, applications, and services) that can be rapidly provisioned and released

with minimal management effort or service provider interaction” [1]. The so-called

cloud service providers (CSPs) are the key players in cloud computing responsible

for providing clients with a wide range of services that vary from applications such

Microsoft Office 365 and Google Docs to a complete infrastructure such as Amazon

Elastic Compute Cloud (EC2) [2]. This introductory section provides the reader with

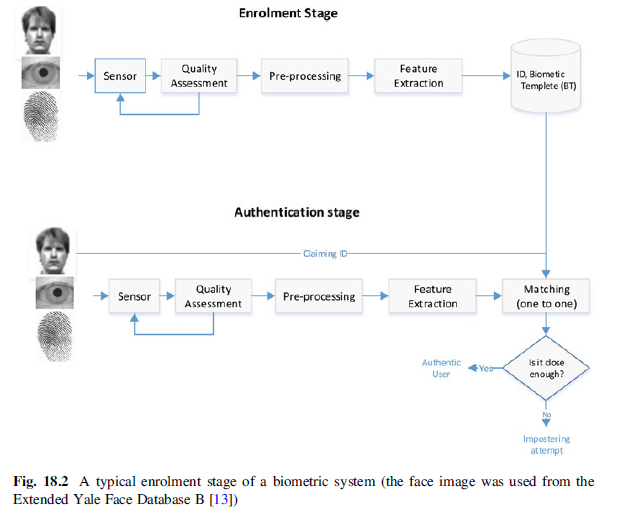
a brief background on four related topics: (1) the main characteristics of cloud

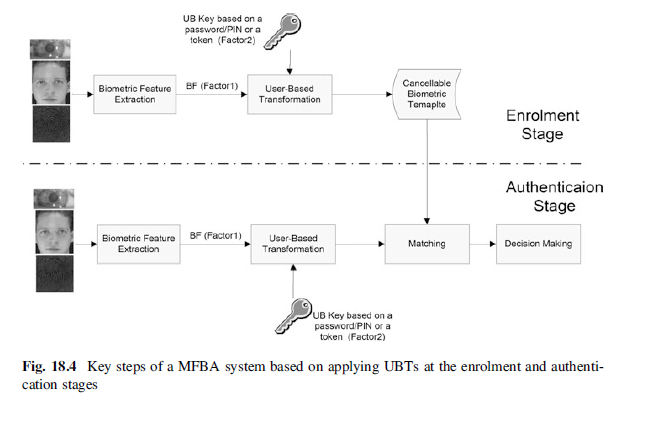
computing, delivery models, and deployment models, (2) security challenges in

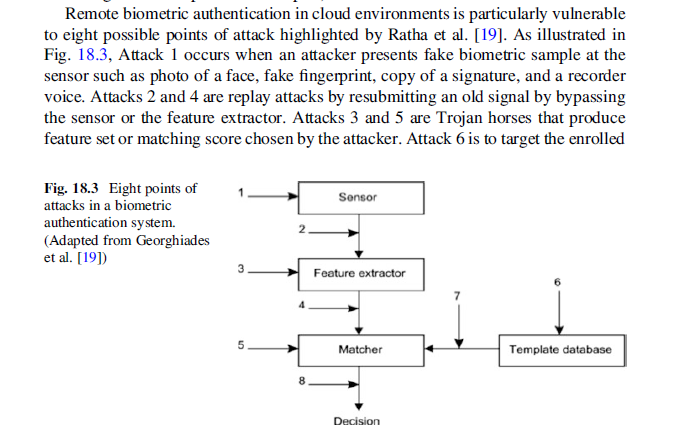
cloud computing, (3) **biometric-based recognition, and (4) the limitations of conventional**

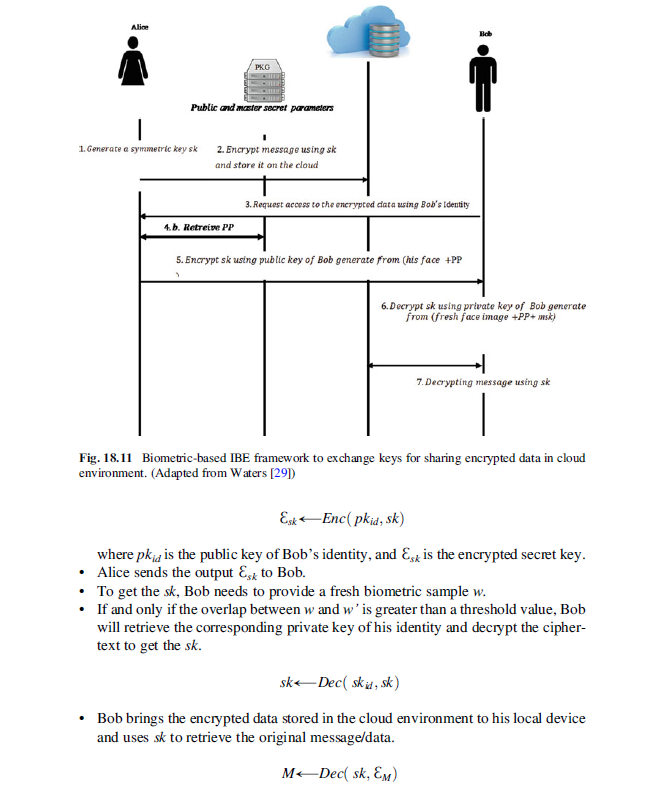
**biometric solutions for remote cloud authentication.**

**Contribution-**









**Limitation-** there is an urgent need for

new legislation to enforce privacy-aware measures on cloud service providers

related to biometric collection, data processing, and template storage. Although

some types of regulation related to users’ privacy and data protection do exist in

many countries, many of these regulations related to managing the privacy and

security of biometric data are either not there yet or insufficient

13.Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment

IEEE,2018

A14

**@article{das2018biometrics,**

**title={Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment},**

**author={Das, Ashok Kumar and Wazid, Mohammad and Kumar, Neeraj and Vasilakos, Athanasios V and Rodrigues, Joel JPC},**

**journal={IEEE Internet of Things Journal},**

**volume={5},**

**number={6},**

**pages={4900--4913},**

**year={2018},**

**publisher={IEEE}**

**}**

**Abstract-** Due to the widespread popularity of Internetenabled

devices, Industrial Internet of Things (IIoT) becomes

popular in recent years. However, as the smart devices share the

information with each other using an open channel, i.e., Internet,

so security and privacy of the shared information remains a

paramount concern. There exist some solutions in the literature

for preserving security and privacy in IIoT environment.

However, due to their heavy computation and communication

overheads, these solutions may not be applicable to wide category

of applications in IIoT environment. Hence, in this paper, we

propose a new Biometric-based Privacy Preserving User Authentication

(BP2UA) scheme for cloud-based IIoT deployment.

**BP2UA consists of strong authentication between users and**

**smart devices using pre-established key agreement between smart**

**devices and the gateway node**. The formal security analysis of

BP2UA using the well-known ROR model is provided to prove its

session key security. Moreover, an informal security analysis of

BP2UA is also given to show its robustness against various types

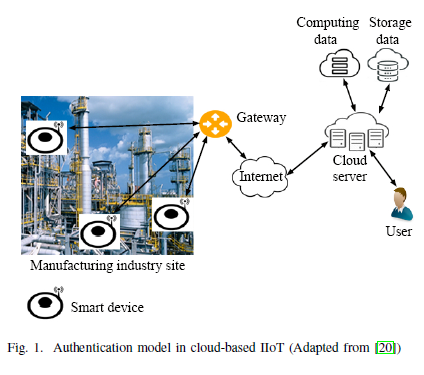
of known attacks. The computation and communication costs

of BP2UA in comparison to the other existing schemes of its

category demonstrate its effectiveness in the IIoT environment.

Finally, the practical demonstration of BP2UA is also done using

the NS2 simulation.

**Contribution-**

Less communication cost,computation cost,

**Limitation-** Packet loss rate is high

### 14.[A multimodal **biometric authentication** scheme **based** on feature fusion for improving security in **cloud** environment](https://link.springer.com/article/10.1007/s12652-020-02184-8)

Springer,2021

a15

**@article{joseph2021multimodal,**

**title={A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment},**

**author={Joseph, Teena and Kalaiselvan, SA and Aswathy, SU and Radhakrishnan, R and Shamna, AR},**

**journal={Journal of Ambient Intelligence and Humanized Computing},**

**volume={12},**

**number={6},**

**pages={6141--6149},**

**year={2021},**

**publisher={Springer}**

**}**

**Abstract-** In recent days, due to the advent of advanced technologies such as cloud computing, accessing data can be done anywhere at

any time. Meanwhile, ensuring the data security is highly significant. Authentication plays a major role in preserving security

via different access control mechanisms. As a recent trend, the biological information of the individual user is considered

as verification scheme for the authentication process. Traits such as fingerprint, iris, ear or palm print are widely used to

develop the authentication systems from its patterns. But, to increase the complexity of the user authentication and to ensure

high security, more than a trait is combined together. In this paper, a multimodal authentication system is proposed by fusing

the feature points of fingerprint, iris and palm print traits. Each trait has undergone the following procedures of image

processing techniques such as **pre-processing, normalization and feature extraction.** From the extracted features, **a unique**

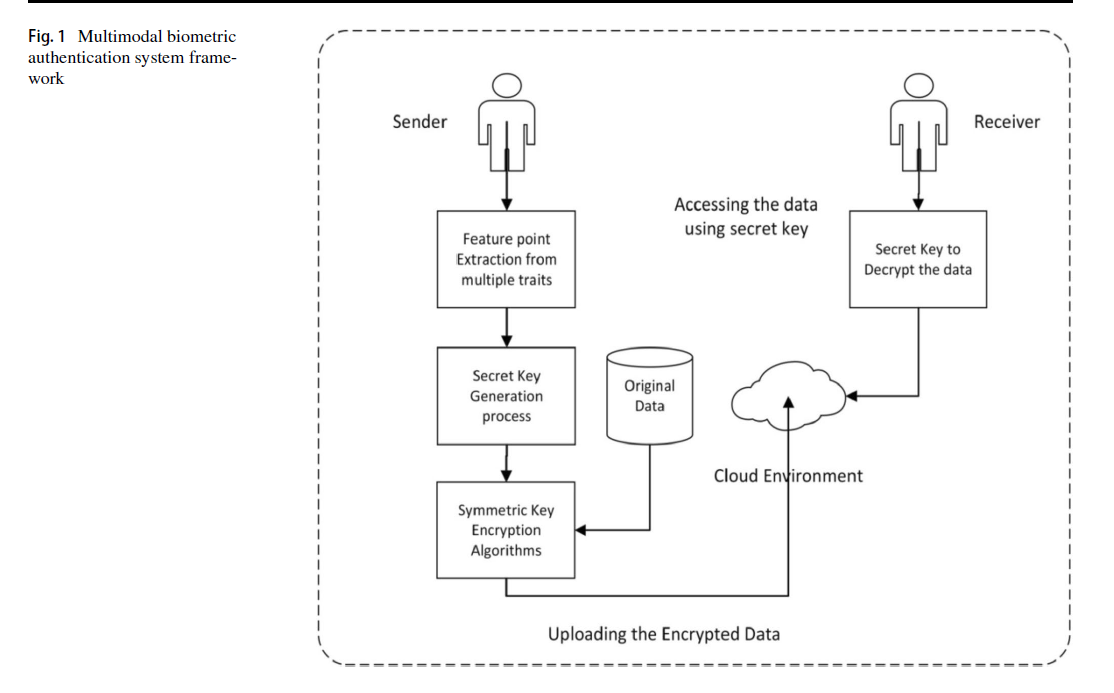
**secret key is generated by fusing the traits in two stages**. False Acceptance Rate (FAR) and False Rejection Rate (FRR)

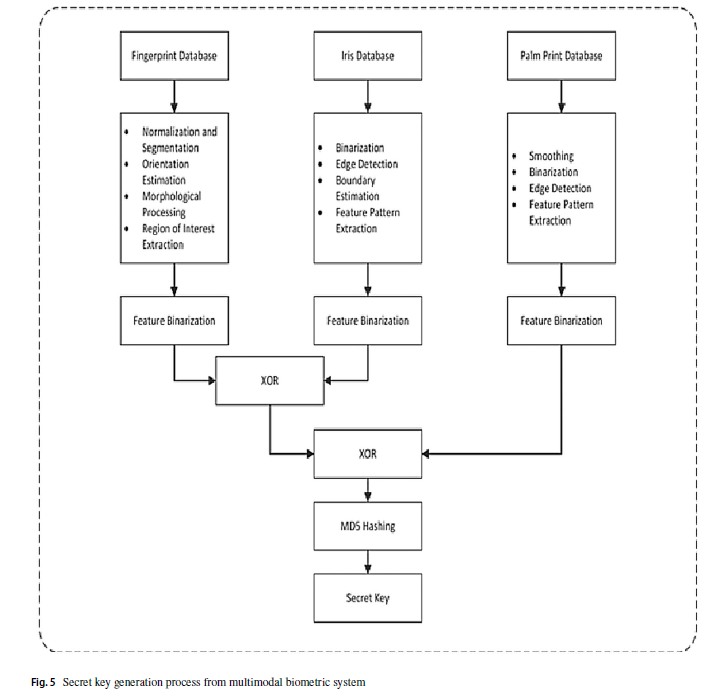
metrics are used to measure the robustness of the system. This performance of the model is evaluated using three standard

symmetric cryptographic algorithms such as AES, DES and Blowfish. This proposed model provides better security and

access control over data in cloud environment.

**Contribution-**

****

****

**Limitation-**

**15.Biometric authentication and image encryption for image security**

**in cloud framework**

**Springer 2019**

**@article{kakkad2019biometric,**

**title={Biometric authentication and image encryption for image security in cloud framework},**

**author={Kakkad, Vishruti and Patel, Meshwa and Shah, Manan},**

**journal={Multiscale and Multidisciplinary Modeling, Experiments and Design},**

**volume={2},**

**number={4},**

**pages={233--248},**

**year={2019},**

**publisher={Springer}**

**}**

**Abstract-** Cloud computing is a major blooming technology which has numerous applications in today’s market and is rightly so hyped.

Images are a major part of today’s internet data traffic, especially due to widespread social media, and hence, its security

is crucial. However, in the present scenario, the images in cloud are a major issue in terms of security. Since the user who

has uploaded the image has no control over the security of images, the cloud provider has to ensure maximum security in

terms of authentication and prevention from attacks. The main objective of this paper is to provide a method to enhance the

safety of images on cloud. This paper presents an idea of securing images on cloud platform using biometric authentication.

Different steps involved in biometric authentication and secure upload and access of images are explained, and integration

of all the steps is done at the end as a case study which puts light on the whole process in which methods are best-regarding

results and compatibility. The proposed algorithm in this paper **presents the idea of authentication of images in two basic**

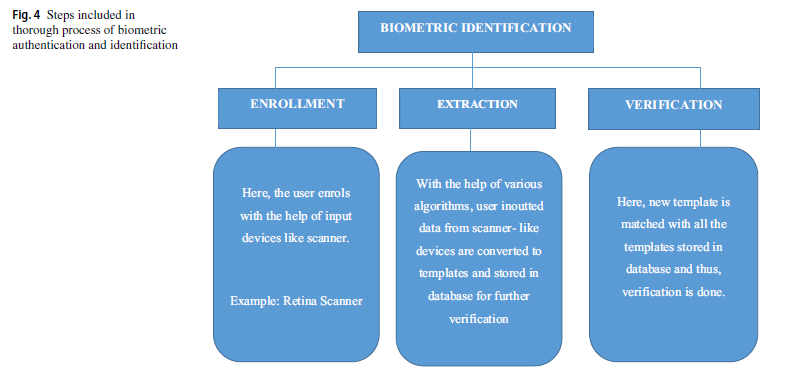
**steps of image compression using standard discrete wavelet transform method followed by image encryption using the hybrid**

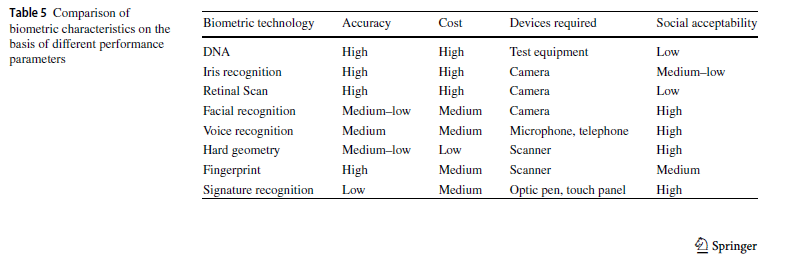
**method of SHA and blowfish. T**his image is then stored into the database of cloud and accessed whenever the user requests

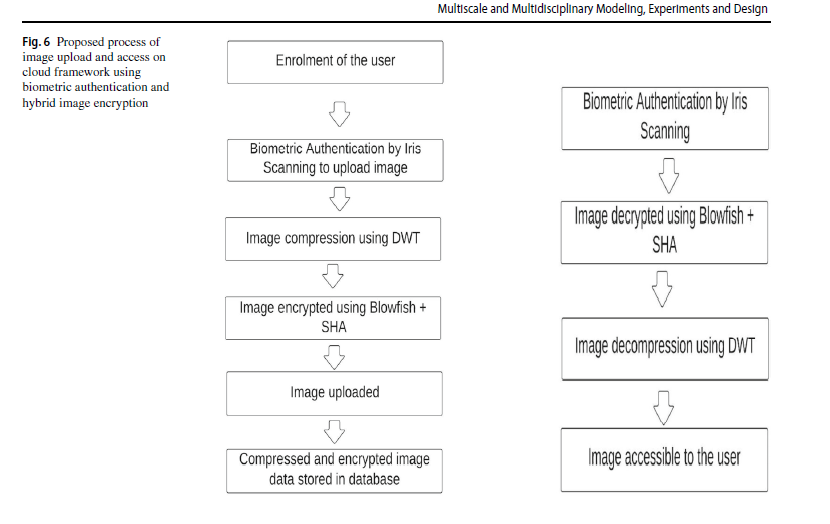
it. A structured and comprehensive view of encryption methods, types of biometrics and to secure data as well as images is

provided in this paper

**Contribution-**

****

****

****

**Limitation-** One of the aims of future research would be to put forth

an algorithm which is more efficient in terms of space and

time complexity. This would lead to an efficient and trustable

cloud network that not only would be user friendly but also

fast and cost-effective

**16.A Smart Biometric Identity Management Framework**

**for Personalised IoT and Cloud Computing-Based**

**Healthcare Services**

**Sensor,2021**

**A17**

**@article{farid2021smart,**

**title={A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services},**

**author={Farid, Farnaz and Elkhodr, Mahmoud and Sabrina, Fariza and Ahamed, Farhad and Gide, Ergun},**

**journal={Sensors},**

**volume={21},**

**number={2},**

**pages={552},**

**year={2021},**

**publisher={MDPI}**

**}**

**Abstract-**This paper proposes a novel identity management framework for Internet of Things (IoT)

and cloud computing-based personalized healthcare systems. The proposed framework uses multimodal

encrypted biometric traits to perform authentication. **It employs a combination of centralized**

**and federated identity access techniques along with biometric based continuous authenticati**on. The

framework uses a fusion of electrocardiogram (ECG) and photoplethysmogram (PPG) signals when

performing authentication. In addition to relying on the unique identification characteristics of the

users’ biometric traits, the security of the framework is empowered by the use of Homomorphic

Encryption (HE). The use of HE allows patients’ data to stay encrypted when being processed or

analyzed in the cloud. Thus, providing not only a fast and reliable authentication mechanism,

but also closing the door to many traditional security attacks. The framework’s performance was

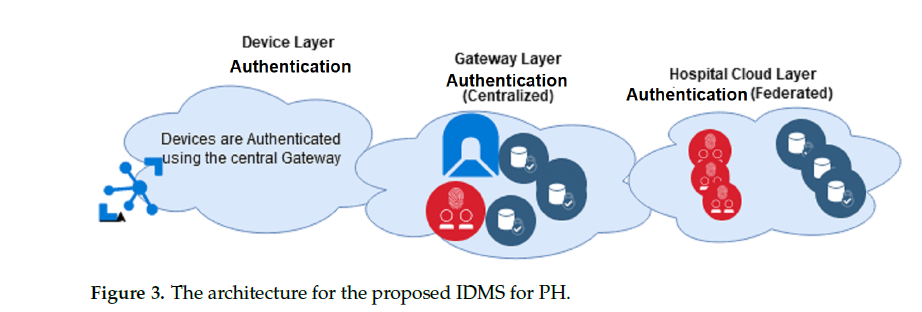
evaluated and validated using a machine learning (ML) model that tested the framework using a

dataset of 25 users in seating positions. Compared to using just ECG or PPG signals, the results of

using the proposed fused-based biometric framework showed that it was successful in identifying

and authenticating all 25 users with 100% accuracy. Hence, offering some significant improvements

to the overall security and privacy of personalized healthcare systems.

**Contribution-**

**Limitation-** End-to-end security has not

been validated. Thus, classical identity-based security attacks, such as man in the middle

and replay attacks, are yet to be tested.

the dataset used to conduct the experiment sourced the PPG and ECG signals

from users in sitting postures. Future work will look into evaluating the performance of the

proposed model in authenticating users while they are in various positions e.g., walking or

climbing stairs.

**17.A survey on Biometric Based Authentication in cloud**

**computing**

**IEEE,2016**

**a3**

**@INPROCEEDINGS{7823273, author={Padma, P. and Srinivasan, S.}, booktitle={2016 International Conference on Inventive Computation Technologies (ICICT)}, title={A survey on biometric based authentication in cloud computing}, year={2016}, volume={1}, number={}, pages={1-5}, doi={10.1109/INVENTIVE.2016.7823273}}**

**Abstract-**The biometric authentication

is broadly classified into physical based biometric authentication

and behavioral based biometric authentication. This paper

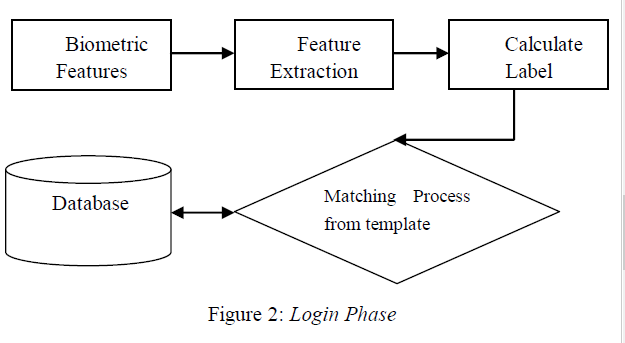
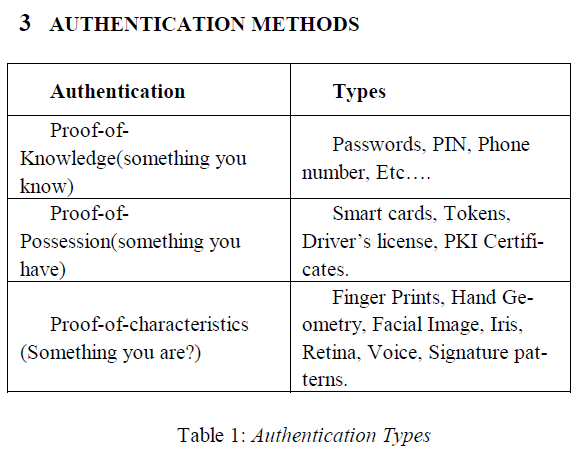
presents an overview of those methods and analyzes their merits

and demerits. The study has been structured to analyze the prevailing

biometric authentication mechanisms to gain insights in developing

a new authentication model that is more efficient than the

existing methods.

**Contribution-**

**Limitation-** Moreover, the behavioral biometric traits are more prone to be

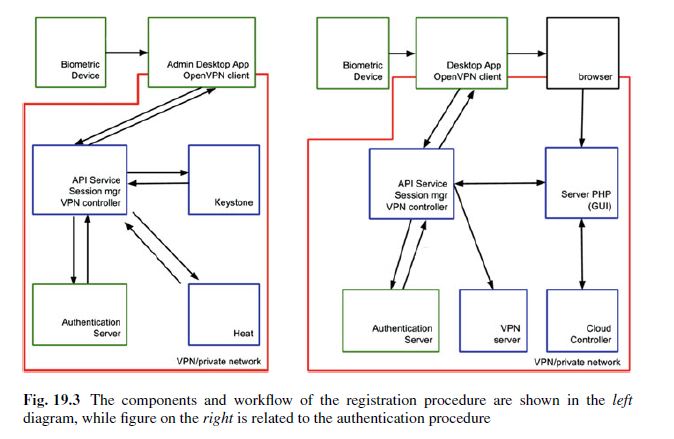
affected by psychological variances of the individual user rather

than the physical traits

**18.Biometric Authentication and Data Security**

**in Cloud Computing**

**Springer,2017**

****

**Architecture of the System**

The architecture of the solution is comprised of interconnected nodes where files

and directories reside. There are two types of nodes: the master node that manages

the filesystem namespace and regulates client access to files, and the slave node

that stores data as blocks within files. All nodes communicate with each other using

TCP-based protocols. The mechanism of data protection does not rely on RAID

approaches, but the file content is replicated on multiple slaves for reliability.Master

and slave nodes can run in a decoupled manner across heterogeneous operating

systems, and on different cloud providers. The complete control of the system is

delegated to the master node, which maintains the namespace tree and the mapping

of blocks to slave nodes. Slave nodes have little intelligence and not know the

location of other slaves or chunks of data.

User applications access the system using a specific client, a library that exports

the filesystem interface. When a user wants to perform a reading action on

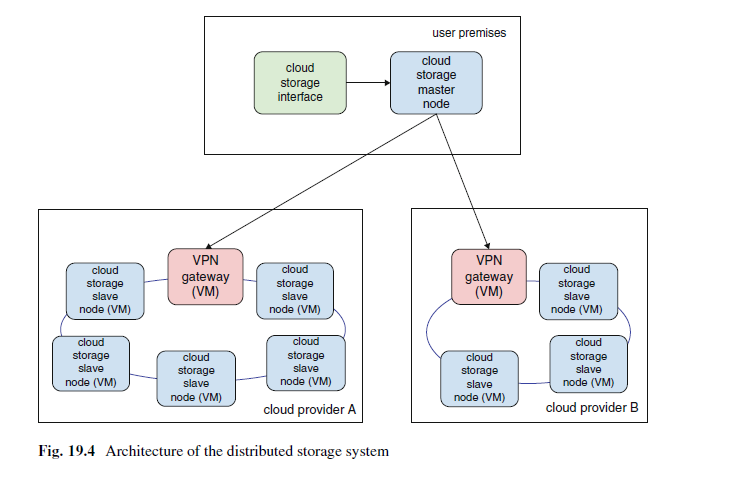
filesystem, the client first asks the master node for the list of namenodes that host the

chunks of the file. After that, the client contacts a slave node directly and requests the

transfer of the desired block. Instead, when a user wants to write on the filesystem,

it first asks the master to choose slaves to host chunks of the file. All decisions

concerning replication of the chunks are taken by the master node. This ensures the

reliability of the data and the fault tolerance of the system.

SOFTWARE AGENTS

19.Modeling and Implementation of Software Agents Decision Making

Ieee,2004

a36

**@INPROCEEDINGS{1327483, author={Far, B.H.}, booktitle={Proceedings of the Third IEEE International Conference on Cognitive Informatics, 2004.}, title={Modeling and implementation of software agents decision making}, year={2004}, volume={}, number={}, pages={258-267}, doi={10.1109/COGINF.2004.1327483}}**

**Abstract-**Software agents are knowledgeable, autonomous,

situated and interactive software entities. Agents’

interactions are of special importance when a group of

agents interact with each other to solve a problem that

is beyond the capability and knowledge of each

individual. Efficiency, performance and overall quality

of the multi-agent applications depend mainly on how

the agents interact with each other effectively. In this

paper, **we suggest an agent model by which we can**

**clearly distinguish different agent’s interaction**

**scenarios.** The model has five attributes: goal, control,

interface, identity and knowledge base. Using the

model, we analyze and describe possible scenarios;

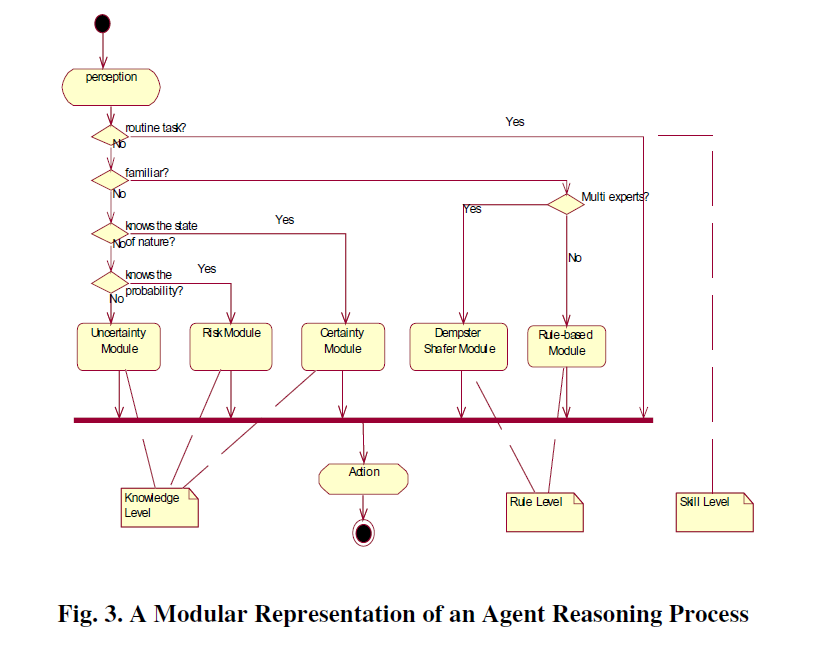
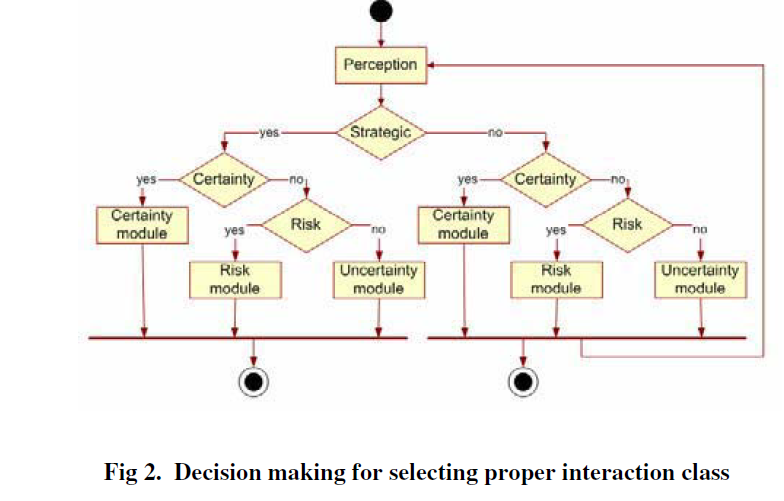
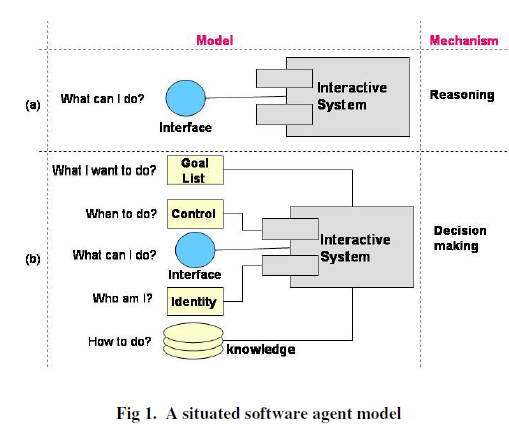
devise the appropriate reasoning and decision making

techniques for each scenario; an**d build a library of**

**reasoning and decision making modul**es that can be

used readily in the design and implementation of

multiagent systems.

**Contribution-**

**Limitation-**

**20.The intelligent agent-based information security model for cloud 2019,ijariit**

**a37**

**@inproceedings{Deshkar2021TheIA,**

**title={The intelligent agent-based information security model for cloud},**

**author={Milind Deshkar},**

**year={2021}**

**}**

**Abstract-** Today’s era is the era of cloud computing and agent-based

processing. Data security and integrity are achieved by

information security systems, which ensure the continuity of

business and protect organizations against potential risks.

Information security systems are used to estimate the risks

and search the place of the occurrence of the risks. It should

also be able to measure the risk consequences associated

with cloud organizations. The cloud organizations must

analyse the information system processes and they should

develop their own information systems based on the analysis.

This paper proposes a comprehensive Agent-Based

Information Security framework for Cloud Computing. We

have considered **risk assessment methods** for calculating

consequences by focussing on potential threats, assets,

vulnerabilities, and their associated measures. A decision

system for the organizations is created by taking the help of

**intelligent (smart) and software agents that are used to fetch**

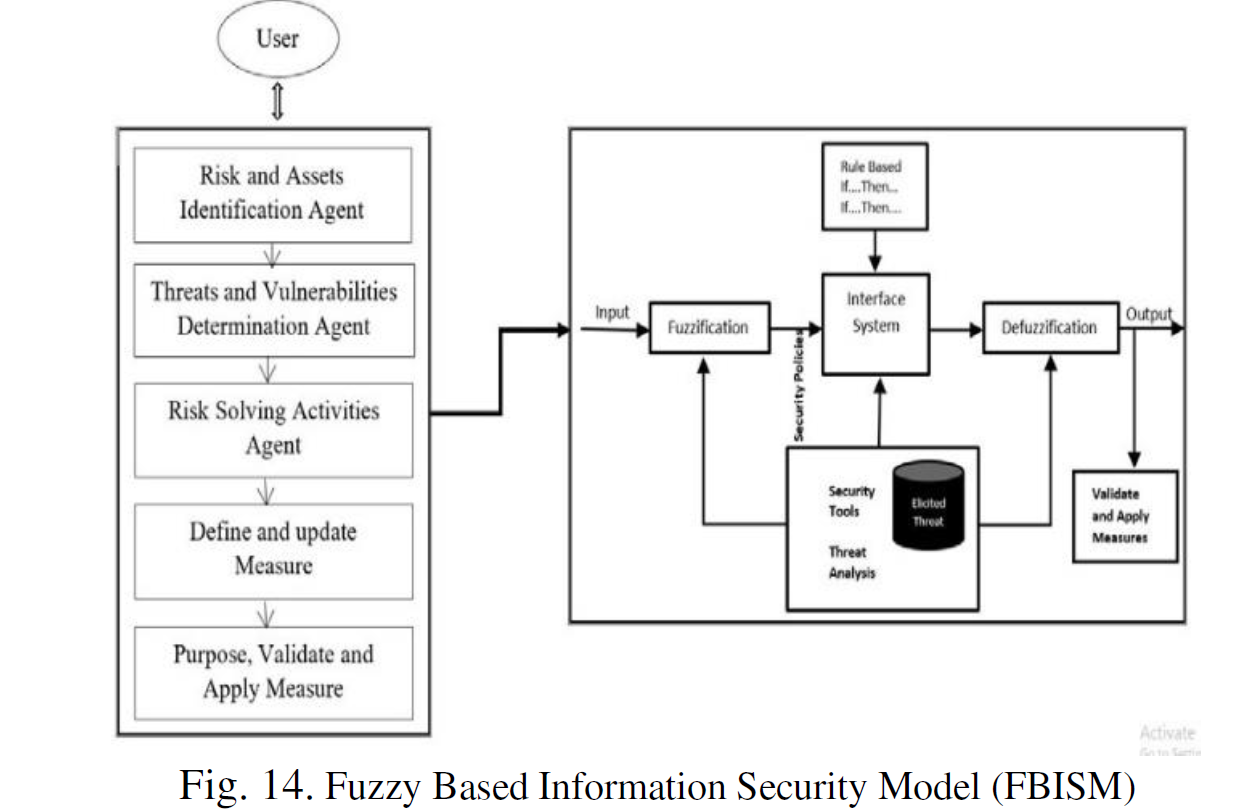
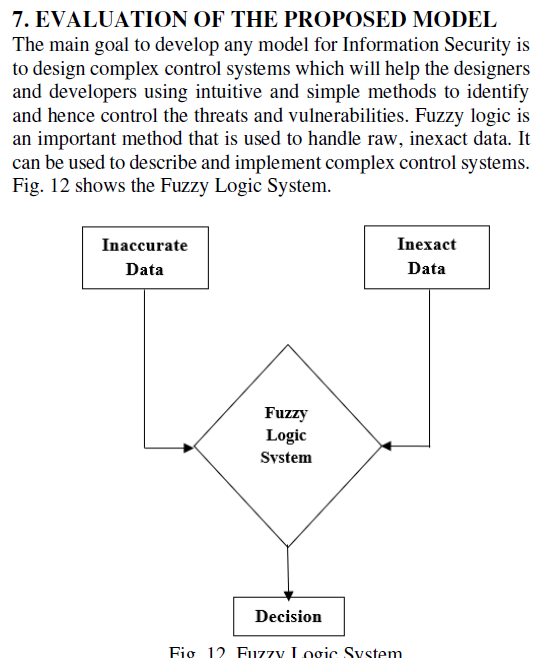
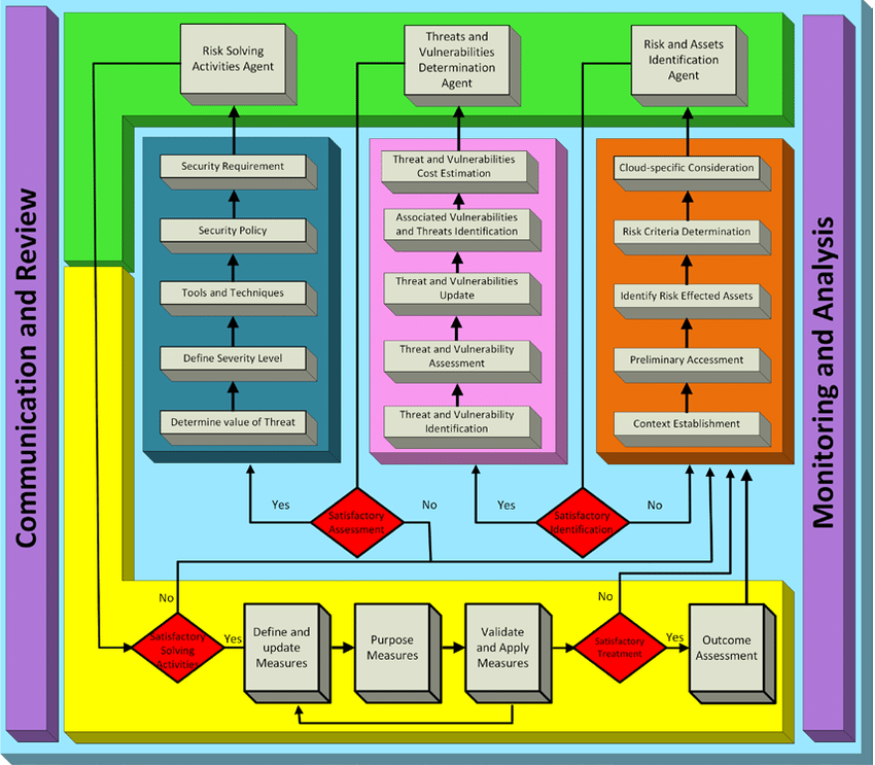
**and group the relevant information used in a framework that**

**decides against threats based on information provided by the**

**security agents.** We have used a fuzzy inference system based

upon fuzzy set theory for creating a decision system.

**Contribution-**



**21.Clouds Meet Agents Toward Intelligent Cloud Services**

**IEEE,2012**

**@ARTICLE{6159219, author={Talia, Domenico}, journal={IEEE Internet Computing}, title={Clouds Meet Agents: Toward Intelligent Cloud Services}, year={2012}, volume={16}, number={2}, pages={78-81}, doi={10.1109/MIC.2012.28}}**

**Abstract-** Cloud computing systems provide large-scale infrastructures for high performance

computing that can adapt to user and application needs. Multiagent

systems (MASs) comprise interacting agents capable of intelligent behaviour.

Integrating these two technologies could enable high-performance, complex

systems and intelligent applications, making clouds more flexible and autonomic

and providing MASs with a reliable and scalable computing infrastructure on

which to execute large-scale applications.

**Contribution-**

A computational entity known as a software agent acts on behalf of another entity to carry out a task or realize a specific objective. Agent systems are standalone computer programs that act independently and embody domain knowledge in order to accomplish predetermined objectives. They are built to function in a setting that is always changing and evolving. Autonomy, proactivity, communication and cooperation, bargaining, and learning are just a few of the characteristics that agents often offer.

**Clouds Using Agents**

cloud computing enabled by software agents, which offers solutions built on the creation and development of software agents. These approaches might enhance cloud resources, service administration and discovery, SLA negotiation, and service composition. Clouds may become wiser in their interactions with users and more effective at distributing processing and storage to apps if they used autonomous agents.Large-scale data centres contain enormous amounts of information that agents may search, filter, query, and update. We might picture a situation in which cloud agents provide intelligent data access and monitoring services on behalf of users and their operating systems, implement processor-to-application assignment schemes, and support the energy-efficient usage of cloud computing infrastructures.Implementing cloud interoperability may benefit from it. Last but not least, because data and software are stored, accessed, and used on devices that are not directly owned by data and software owners, security and trust are crucial cloud computing challenges. Decentralised and scalable solutions for trust and security in cloud infrastructures can be offered via agent-based models and algorithms.

**Limitation-**

**22.Software Agents: Characteristics and Classification**

**@inproceedings{MahmoudAgentsC,**

**title={Agents : Characteristics and Classification},**

**author={Qusay H. Mahmoud}**

**}**

**Abstract-** Since the arrival of the World-Wide Web, and the explosive growth of

information on the Web, researchers in the field of Software Agents got interested in

information agents (also known as Internet agents). However, for the past couple of

years, agent technology has been a hot topic, and most likely, this is mainly due to

the popularity of the Java programming language, which represents an ideal

language for implementing software agents as it is the “Write Once Run Anywhere”

language. This is an important feature for software agents as it allows them to run on

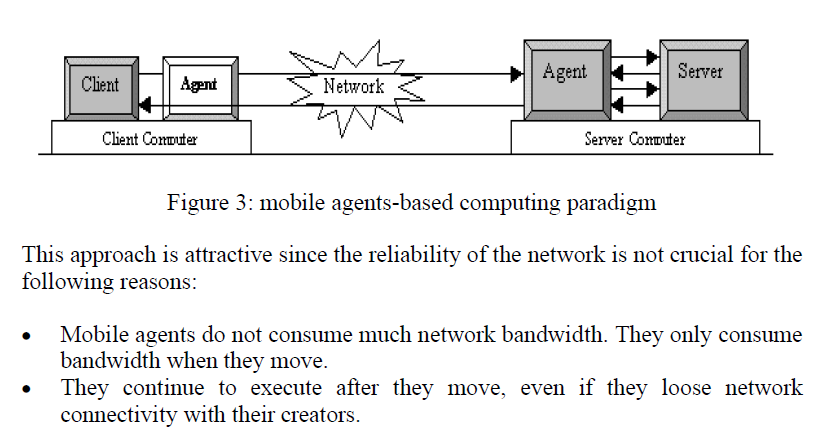
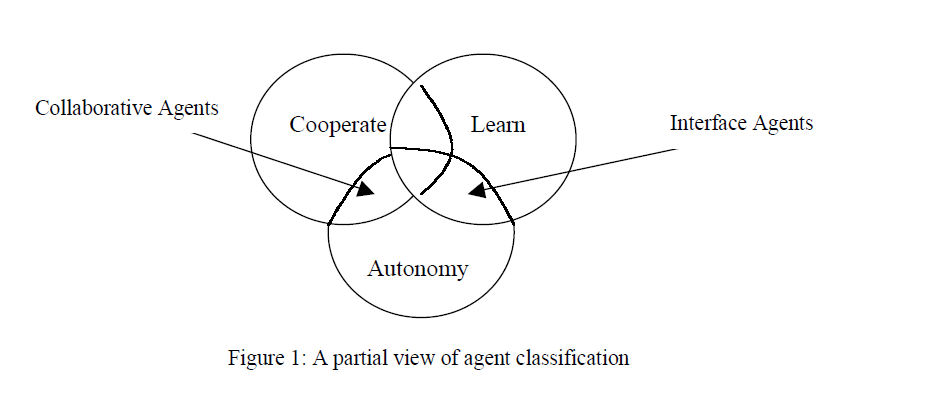
all platforms of the Internet. The word “agent” however, has been misused. People

involved in agent research have a variety of definitions for that word. This paper

presents a brief overview of software agents, with emphasis on mobile agents. We

classify agents in different types along several primary characteristics that agents

should exhibit.

**Contribution-** 

23.Survey of agent-based cloud computing applications

2019,Elsevier

a38

**@article{de2019survey,**

**title={Survey of agent-based cloud computing applications},**

**author={De la Prieta, Fernando and Rodr{\'\i}guez-Gonz{\'a}lez, Sara and Chamoso, Pablo and Corchado, Juan Manuel and Bajo, Javier},**

**journal={Future generation computer systems},**

**volume={100},**

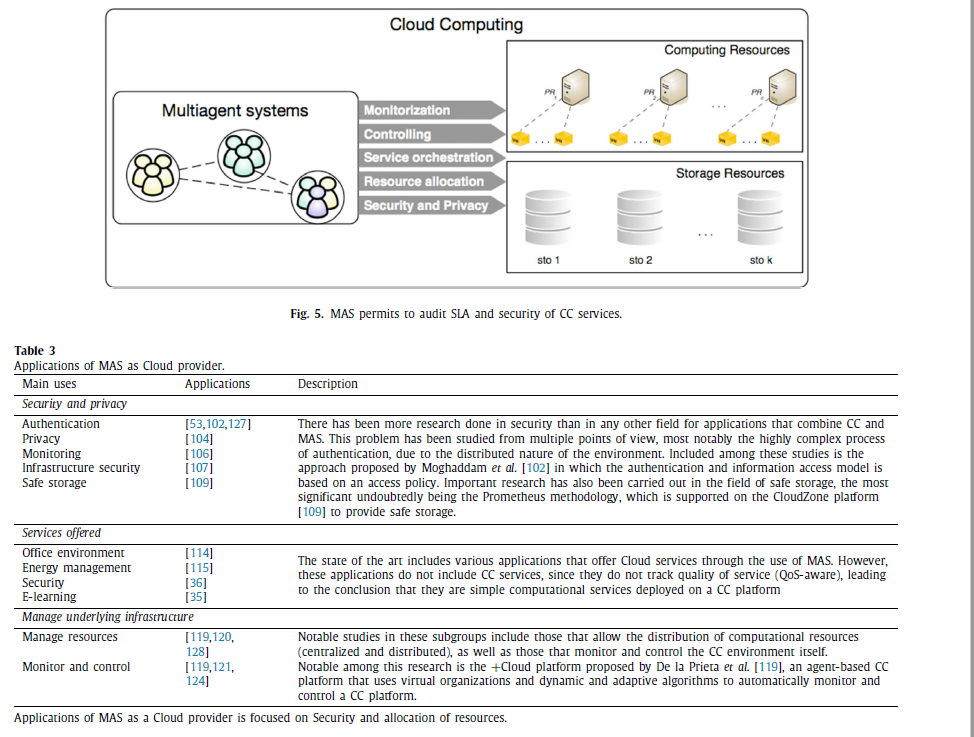
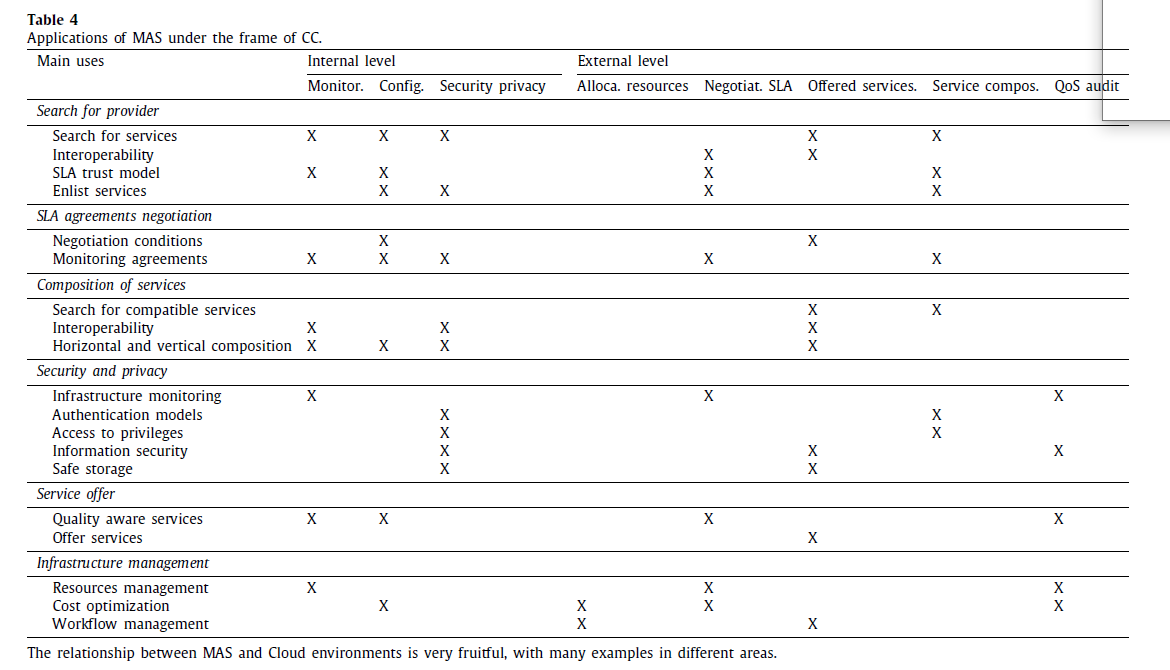
**pages={223--236},**

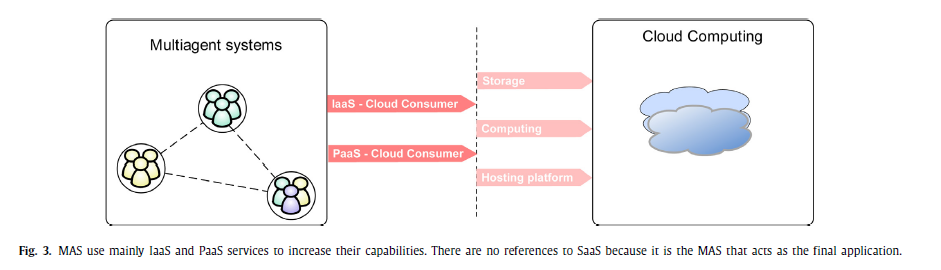
**year={2019},**

**publisher={Elsevier}**

**}**

**Abstract-** In the state of the art, there are very few studies on agent-based Cloud Computing. Nevertheless, this is an emerging trend and the number of studies and applications in this field is beginning to increase. Cloud Computing and Agents are complementary technologies. The features of Cloud Computing can provide advanced computational characteristics to multi-agent systems. In turn, the inclusion of agent systems in the core of the Cloud platform makes it possible to incorporate different functionalities, such as reasoning and learning capabilities. This study analyzes the emerging relationship between both distributed systems. Specifically, this study proposes a new classification from the point of view of Cloud Computing, based on the reference architecture proposed by the National Institute of Standards and Technology and the different responsibilities of each of the roles that participate in the Cloud Computing paradigm as identified in the architecture: Provider, Consumer, Broker, Carrier and Auditor.

**Contribution-** 



**24.Agent Based Information Security Framework for Hybrid Cloud Computing**

**2019,KSII Transactions on Internet and Information Systems**

**@article{tariq2019agent,**

**title={Agent based information security framework for hybrid cloud computing},**

**author={Tariq, Muhammad Imran},**

**journal={KSII Transactions on Internet and Information Systems (TIIS)},**

**volume={13},**

**number={1},**

**pages={406--434},**

**year={2019},**

**publisher={Korean Society for Internet Information}**

**}**

**a40**

**Abstract-** In general, an information security approach estimates the risk, where the risk is to occur due to an unusual event, and the associated consequences for cloud organization. Information Security and Risk Management (ISRA) practices vary among cloud organizations and disciplines. There are several approaches to compare existing risk management methods for cloud organizations but their scope is limited considering stereo type criteria, rather than developing an agent based task that considers all aspects of the associated risk. It is the lack of considering all existing renowned risk management frameworks, their proper comparison, and agent techniques that motivates this research. This paper proposes Agent Based Information Security Framework for Hybrid Cloud Computing as an all-inclusive method including cloud related methods to review and compare existing different renowned methods for cloud computing risk issues and by adding new tasks from surveyed methods. **The concepts of software agent and intelligent agent have been introduced that fetch/collect accurate information used in framework and to develop a decision system that facilitates the organization to take decision against threat agent on the basis of information provided by the security agents.** The scope of this research primarily considers risk assessment methods that focus on assets, potential threats, vulnerabilities and their associated measures to calculate consequences. After in-depth comparison of renowned ISRA methods with ABISF, we have found that ISO/IEC 27005:2011 is the most appropriate approach among existing ISRA methods. The proposed framework was implemented using fuzzy inference system based upon fuzzy set theory, and MATLAB® fuzzy logic rules were used to test the framework. The fuzzy results confirm that proposed framework could be used for information security in cloud computing environment.

**Contribution-**

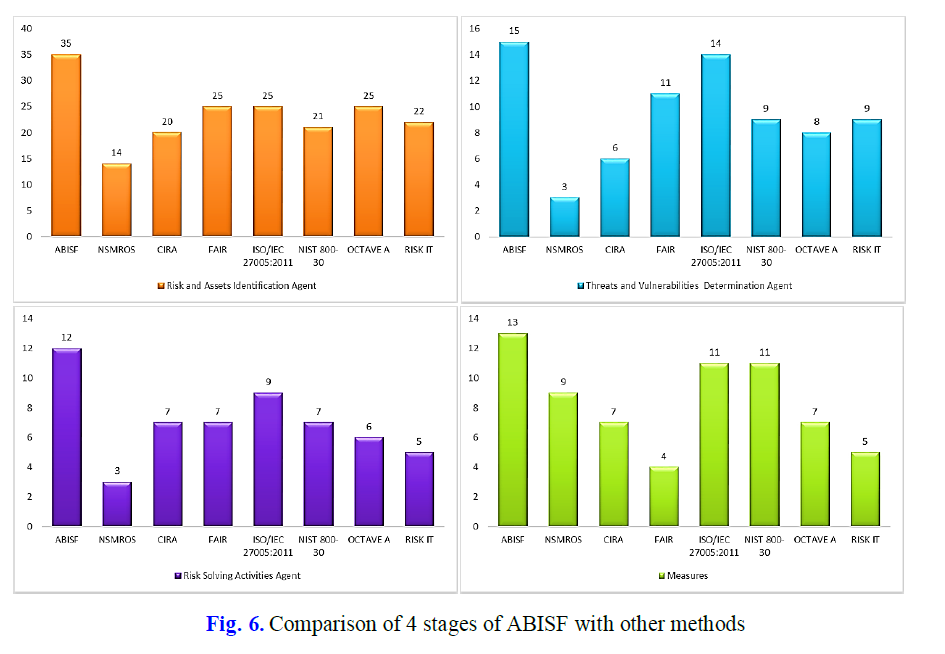
The main advantages of the agent-based systems are:

1. The network load is significantly reduced

2. The network latency is greatly reduced

3. The system becomes robust

4. Adapt dynamically and fault tolerant



**Limitation-**  The study had several limitations that our future efforts can address. Let’s say, we had studied seven Information Security Risk Assessment methods while during literature review, we found some other methods that we did not discuss in this paper. Furthermore, a number of researchers proposed their own ISRA methods that we did not consider. Second limitation is that the authors are novices, thus the ISRA experts may differ from the results. However, these results will be a guideline and prove useful for non-specialists and novices.

**25.An approach for the secure management of hybrid cloud–edge**

**environments**

**2018,Elsevier**

**a35**

**@article{article,**

**author = {Celesti, Antonio and Fazio, Maria and Galletta, Antonino and Carnevale, Lorenzo and Wan, Jiafu and Villari, Massimo},**

**year = {2018},**

**month = {07},**

**pages = {},**

**title = {An approach for the secure management of hybrid cloud-edge environments},**

**volume = {90},**

**journal = {Future Generation Computer Systems},**

**doi = {10.1016/j.future.2018.06.043}**

**}**

**Abstract-** The Cloud-of-Things (CoT) paradigm is a challenging approach to manage IoT applications exploiting Cloud resources and services. In order to avoid latency in Cloud–IoT communications, the management of time-sensitive services has to be moved to the edge of the CoT. To this aim, a secure Cloud-to-Edge environment for seamless management of IoT applications is necessary. The realization of a performing and secure Cloud-to-Edge middleware solution is a very strategic goal for future business CoT services. Thus, it needs to be deeply investigated, as highlighted by the **Cloud Security Alliance (CSA)**. A valuable approach to develop an efficient Cloud-to-Edge system is based on an instant-message communication solution. In current Cloud environments, a Message Oriented Middleware (MOM) based on an Instant Message Protocol (IMP) provides good performance, but overlook security requirements. **In this paper, we aim at overcoming such a gap following the CSA guidelines. In particular, we discuss the involved issues for improving such a kind of Cloud-to-Edge system in order to achieve data confidentiality, integrity, authenticity and non-repudiation.** Moreover, we analyze a real case of study considering aMOM architectural model. Experimental results performed on a real testbed show how the introduced secure

capabilities do not affect the overall performances of the whole middleware.

**Contribution-** Cloud and edge layers management

In this Section, we describe the **software agent that allows**

**MOM4Cloud to manage efficiently the Clouds and Edge layers**.

The Cloud/Edge Management Agent belongs to the Host Manager

Agent. Indeed, it is necessary an Agent for managing each

host. In order to make the maintenance of the whole middleware

easy, the Cloud/Edge Management Agent is provided by a specific

plugin. The enabling technology of such plugin is jClouds [29]. It

supports more than 30 providers, such as Amazon EC2, Rackspace,

Microsoft Azure, and Application Program Interfaces (APIs) for the

interaction with Virtual Infrastructure Managers (VIMs), such as

OpenStack, and Container Engines, such as Docker.

Fig. 2 shows the sequence diagram for deploying resources into

the Cloud and Edge Layers. 

26.An Analysis of the Interaction Between Intelligent Software

Agents and Human Users

2018,Springer

**@article{burr2018analysis,**

**title={An analysis of the interaction between intelligent software agents and human users},**

**author={Burr, Christopher and Cristianini, Nello and Ladyman, James},**

**journal={Minds and machines},**

**volume={28},**

**number={4},**

**pages={735--774},**

**year={2018},**

**publisher={Springer}**

**}**

**Abstract-** Interactions between an **intelligent software agent (ISA)** and a human user are ubiquitous

in everyday situations such as access to information, entertainment, and purchases.

In such interactions, the ISA mediates the user’s access to the content, or

controls some other aspect of the user experience, and is not designed to be neutral

about outcomes of user choices. Like human users, ISAs are driven by goals, make

autonomous decisions, and can learn from experience. Using ideas from bounded

rationality (and deploying concepts from artificial intelligence, behavioural economics,

control theory, and game theory), we frame these interactions as instances of an

ISA whose reward depends on actions performed by the user. Such agents benefit

by steering the user’s behaviour towards outcomes that maximise the ISA’s utility,

which may or may not be aligned with that of the user. Video games, news recommendation

aggregation engines, and fitness trackers can all be instances of this

general case. **Our analysis facilitates distinguishing various subcases of interaction**

**(i.e. deception, coercion, trading, and nudging), as well as second-order effects that**

**might include the possibility for adaptive interfaces to induce behavioural addiction,**

**and/or change in user belief.** We present these types of interaction within a conceptual

framework, and review current examples of persuasive technologies and the

issues that arise from their use. We argue that the nature of the feedback commonly

used by learning agents to update their models and subsequent decisions could steer

the behaviour of human users away from what benefits them, and in a direction that

can undermine autonomy and cause further disparity between actions and goals as

exemplified by addictive and compulsive behaviour. We discuss some of the ethical,

social and legal implications of this technology and argue that it can sometimes

exploit and reinforce weaknesses in human beings.

**Contribution-**

Coercion

A familiar, mild form of coercion is when the user is in need of information and so

accesses a RS, but cannot skip a promotional video. Since they have no choice (i.e.

their set of actions have been restricted), and were not looking for that video, they

have been coerced to see it. This situation is also commonly found in a variant form:

when other actions are requested as a prerequisite to gaining access to some service

(e.g. sharing personal data in order to gain access).

Deception

As a particular type of deception, consider the case of clickbait, or an ISA that

selects links with misleading descriptions. Clickbait and phishing scams are a form

of deceiving recommendations, which misrepresent their real contents, sometimes

requiring several additional links before that is discovered.

Trading

Trading occurs when the ISA has some knowledge of the user’s goals (either

revealed by their actions, or explicitly stated by the user), and presents the user with

options that are expected to increase both the user’s utility and the ISA’s utility—

both sides benefit from the trade.

Feedback

It is important for an ISA to have information about the goals or needs of the user.

While it is possible to ask them (e.g. to rate or review various products), it is often

more economical to just observe their behaviour and collect information about what

they end up clicking on

Nudging

Nudging occurs when an ISA attempts to induce user engagement without significantly

altering the payoff structure of the options, and without coercion and deception

(Thaler and Sunstein 2008). Nudging is successful because humans are limited

in the resources they can devote to decision-making (e.g. time, information,

and computational resources), and like artificial agents,15 human agents use heuristics

to quickly select a few salient options when making decisions

**Second‑Order Effects**

There are ways in which a human user’s behaviour may be influenced as an unintended

result of interacting with an ISA. While the ISA might be rewarded only for

influencing immediate actions, a side effect of this interaction might result in longterm

changes to either the beliefs or the utilities of the user, which in turn will influence

future decisions as they combine to form the user’s value function. We call

these ‘second-order effects’.

Although their account relies on a formal framework for justification, which is beyond the scope of this article to detail, their argument can be summarised as follows:

• If a software agent can act upon and be acted upon by the environment (e.g. a

user); can change state (according to some rules); and can change its internal

parameters (e.g. changing those rules), then the software will appear interactive,

autonomous, and adaptive.

• These three criteria (i.e. ‘interactivity’, ‘autonomous behaviour’, and ‘adaptivity’),

when specified at an appropriate level of abstraction,34 jointly characterise

what it is to be an agent.

• A moral agent must be capable of performing morally qualifable actions (i.e.

causing moral good or evil).

• Artificial agents, by virtue of their autonomous, interactive, and adaptive behaviour

are also capable of performing morally qualifiable actions.

Image Steganography

**27.Cloud Computing Security Using Steganography**

**2019,jetir**

**a5**

**@article{article,**

**author = {Singh, Santosh and Manjhi, Pankaj and Tiwari, R},**

**year = {2019},**

**month = {06},**

**pages = {923-927},**

**title = {Cloud Computing Security Using Steganography},**

**volume = {VI}**

**}**

**Abstract-** Cloud computing provides the ability to use computing and storage resources on a rented basis and reduce the investments in an organization’s computing infrastructure. With huge benefits cloud computing also brings with it concerns about the security and privacy of information. Now a days cloud computing is used by smart mobile applications so there are some security and privacy concerns on data provided by the cloud providers. **In this paper, we demonstrate how Steganography, which is a secrecy method to conceal information, can be used to enhance the security and privacy of data maintained on the cloud by mobile applications. Our proposed design works with a key**, which is securely surrounded in the image along with the data, to provide an additional layer of security.

**Contribution-**

By masking data or information, steganography enables data or information to be conveyed to the recipient end without them being aware that the original message still exists. The procedures often entail embedding a secret message in a transport medium. Steganography, which converts a message into an unintelligible string that can only be decoded by the receiver end, is completely different from cryptography in that it involves developing and evaluating protocols that prevent third parties or the general public from accessing private messages. Similar to cryptography, it is common for a message to contain data or information, but the message's data or information may have been swapped out. Similar to steganography, the average person is unaware that a message or data in the form of data has been conveyed.

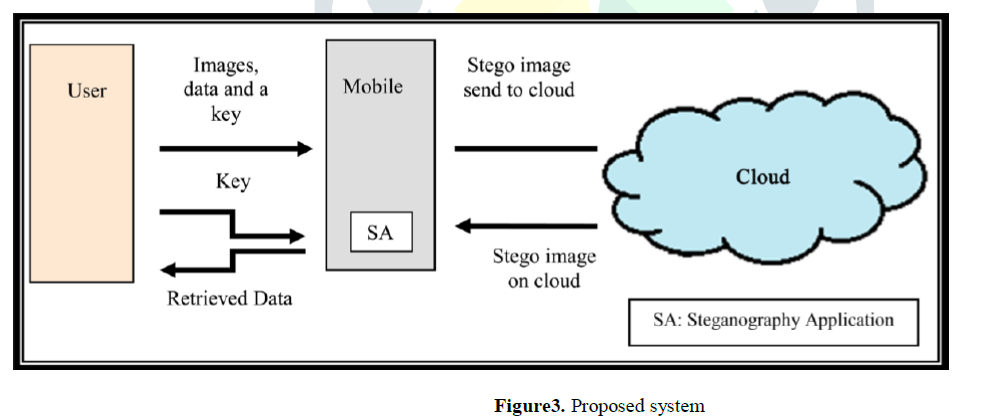
Type of Steganography can be: (1) Steganography (pure), (2) Steganography (symmetric) and (3) steganography (asymmetric) [6]. Steganography (Pure) - any of information no need to exchange. Steganography (Symmetric) - exchange of keys does not require prior to sending the messages.

Steganography (Asymmetric) - exchanging keys does not require prior to sending the messages

Methods of Steganography

Generally most common approaches for information hiding are: (1) Least Significant Bit (LSB) insertion, (2) Masking and filtering techniques, (3) Algorithms and Transformation [4].

LSB



**Limitation-**  The proposed system will work efficiently with the key, but if he/she loses the key, then the system does not have any provision to recover the key, so in this case a user might cause lose the data. This is the serious drawback on which we will work in future. Proposed system is only applicable for limited data.

**28.Image Steganography in Spatial Domain: A Survey**

**July 2018,Elsevier**

**A26**

**@article{hussain2018image,**

**title={Image steganography in spatial domain: A survey},**

**author={Hussain, Mehdi and Wahab, Ainuddin Wahid Abdul and Idris, Yamani Idna Bin and Ho, Anthony TS and Jung, Ki-Hyun},**

**journal={Signal Processing: Image Communication},**

**volume={65},**

**pages={46--66},**

**year={2018},**

**publisher={Elsevier}**

**}**

**Abstract-** This paper presents a literature review of image steganography techniques in the

spatial domain for last 5 years. The research community has already done lots of

noteworthy research in image steganography. Even though it is interesting to

highlight that the existing embedding techniques may not be perfect, the objective of

this paper is to provide **a comprehensive survey and to highlight the pros and cons of**

**existing up-to-date techniques for researchers that are involved in the designing of**

**image steganographic system.** In this article, the general structure of the

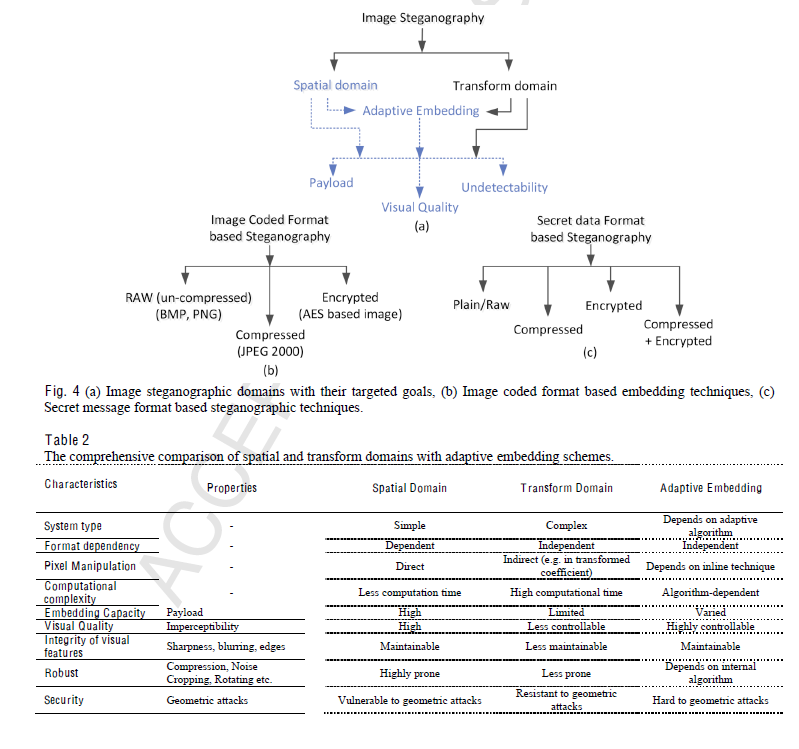
steganographic system and classifications of image steganographic techniques with

its properties in spatial domain are exploited. Furthermore, different performance

matrices and steganalysis detection attacks are also discussed. The paper concludes

with recommendations and good practices drawn from the reviewed techniques.

**Contribution-**



12 methods, Evaluation techniques are included.

**29.Enhancing Image Security and Privacy in Cloud System**

**Using Steganography**

**Wen-Chuan Wu and Shang-Chian Yang**

**2017,IEEE**

**a26**

**@INPROCEEDINGS{7991125, author={Wu, Wen-Chuan and Yang, Shang-Chian}, booktitle={2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)}, title={Enhancing image security and privacy in cloud system using steganography}, year={2017}, volume={}, number={}, pages={321-322}, doi={10.1109/ICCE-China.2017.7991125}}**

**Abstract-** Cloud systems are a popular type of Internet-based

computing that provides shared digital resources to computers

and other devices on demand. Such systems also allow users

uploading and offloading data to the cloud by mobile applications.

There are some potential security and privacy concerns using

mobile devices since cloud systems are usually in a public domain.

**This paper presents an efficient image protection method to**

**secure the existence of important private images in the cloud by**

**using steganography techniqu**e. Experimental results show that

the proposed method is able to not only enhance image security

but also increase the cloud storage capacity.

**Contribution-** This section introduces the proposed method for protecting

individual confidential images over the cloud. It consists of

two procedures: **private image embedding as well as private**

**image extraction.**

**Limitation-**

30.Data Security in Cloud Computing Using Steganography: A Review

Ieee,2019

A6

@INPROCEEDINGS{8646434, author={AlKhamese, Aya Y. and Shabana, Wafaa R. and Hanafy, Ibrahim M.}, booktitle={2019 International Conference on Innovative Trends in Computer Engineering (ITCE)}, title={Data Security in Cloud Computing Using Steganography: A Review}, year={2019}, volume={}, number={}, pages={549-558}, doi={10.1109/ITCE.2019.8646434}}

**Abstract-** Cloud computing is one of the largest

developments in the field of information technology during

recent years. It is a service oriented computing which offers

everything as a service via the internet by the pay-as-you-go

model. It becomes more desirable for all organizations (such

as education, banking, healthcare and manufacturing) and also

for personal use as it provides a flexible, scalable, and reliable

infrastructure and services. For the user, the most important

issue is to store, retrieve and transmit the data over the cloud

network and storage in a secure manner. Steganography and

cryptography are some of the security techniques applied in

the cloud to secure the user data transmitting. The objective of

steganography is to hide the existence of communication from

the unintended users; whereas cryptography encrypts the data

to make it more secure. Steganography is considered as the

most effective technique for securing the communication in

the cloud. Digital images are most commonly used as a cover

medium in steganography. In the literature, there exist several

image steganography techniques for hiding information in

images; which were developed and implemented in the time

domain as well as in the frequency domain. **Fundamentals of**

**spatial domain and frequency domain techniques are reviewed**

**in this paper with emphasis on the Least Significant Bit (LSB)**

**and the Discrete Cosine Transform (DCT) techniqu**es.

**Contribution-** Image steganography techniques

**31.Adaptive Payload Distribution in Multiple Images**

**Steganography Based on Image Texture Features**

**Ieee,2020**

a27

@ARTICLE{9124671, author={Liao, Xin and Yin, Jiaojiao and Chen, Mingliang and Qin, Zheng}, journal={IEEE Transactions on Dependable and Secure Computing}, title={Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features}, year={2022}, volume={19}, number={2}, pages={897-911}, doi={10.1109/TDSC.2020.3004708}}

**Abstract-** With the coming era of cloud technology, cloud storage is an emerging technology to store massive digital images, which provides

steganography a new fashion to embed secret information into massive images. Specifically, a resourceful steganographer could embed a set

of secret information into multiple images adaptively, and share these images in cloud storage with the receiver, instead of traditional single

image steganography. Nevertheless, it is still an open issue how to allocate embedding payload among a sequence of images for security

performance enhancement. **This paper formulates adaptive payload distribution in multiple images steganography based on image texture**

**features and provides the theoretical security analysis from the steganalyst’s point of view.** Two payload distribution strategies based on image

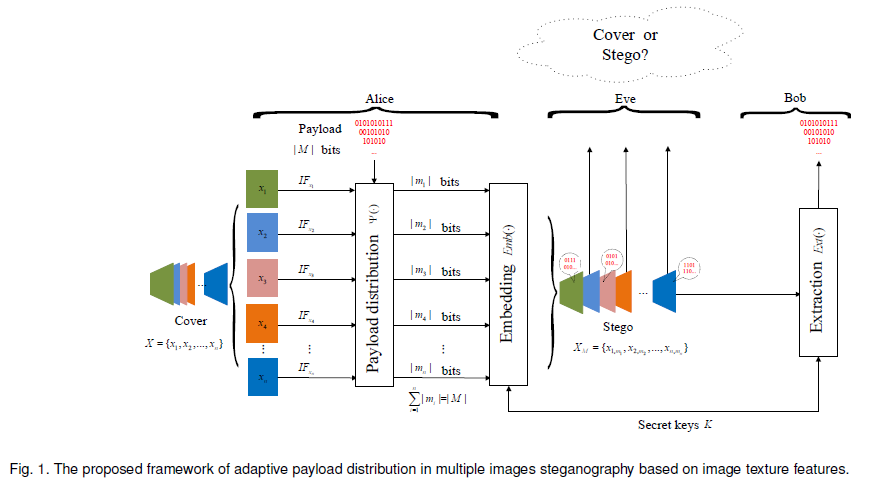
texture complexity and distortion distribution are designed and discussed respectively. The proposed strategies can be employed together with

these state-of-the-art single image steganographic algorithms. The comparisons of the security performance against the modern universal

pooled steganalysis are given. Furthermore, this paper compares the per image detectability of these multiple images steganographic

schemes against the modern single image steganalyzer. Extensive experimental results show that the proposed payload distribution

strategies could obtain better security performance.

**Contribution-**  ESITC assigns the amount of the sub-payload in each image, according to the image capacity derived from image texture complexity. The payload is embedded into as few images as possible, and the

sub-payload of each image is equal to its estimated capacity. ESDD strategy allocates the sub-payload depending on the statistical distribution of embedding distortion values, which are related to statistical detectability of embedding changes.

32.Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research

2019,Elsevier

A7

@article{kadhim2019comprehensive,

title={Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research},

author={Kadhim, Inas Jawad and Premaratne, Prashan and Vial, Peter James and Halloran, Brendan},

journal={Neurocomputing},

volume={335},

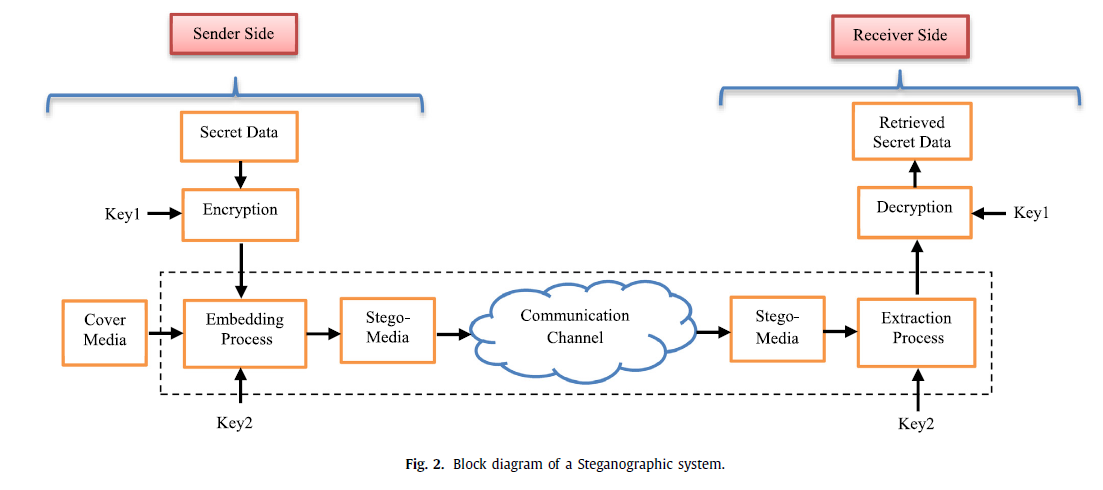
pages={299--326},

year={2019},

publisher={Elsevier}

}

**Abstract-** Storing and communicating secret and/or private information has become part of our daily life whether it is for our employment or personal well-being. Therefore, secure storage and transmission of the se- cret information have received the undivided attention of many researchers. The techniques for hiding confidential data in inconspicuous digital media such as video, audio, and image are collectively termed as Steganography. Among various media types used, the popularity and availability of digital images are high and in this research work and hence, our focus is on implementing digital image steganography. The main challenge in designing a steganographic system is to maintain a fair trade-off between robust- ness, security, imperceptibility and higher bit embedding rate. **This research article provides a thorough review of existing types of image steganography and the recent contributions in each category in multi- ple modalities.** The article also provides a complete overview of image steganography including general operation, requirements, different aspects, different types and their performance evaluations. Different performance analysis measures for evaluating steganographic systems are also discussed here. Moreover, we also discuss the strategy to select different cover media for different applications and a few state-of- the-art steganalysis systems.

**Contribution-** 

Properties of steganography

There are mainly three essential properties of any stegano- graphic systems, namely **imperceptibility, security and capacity** of hiding information [36,37] . While [35,38–40] in their research mentioned that there are four properties, same pervious proper- ties along with **robustness** .

Performance evaluation techniques

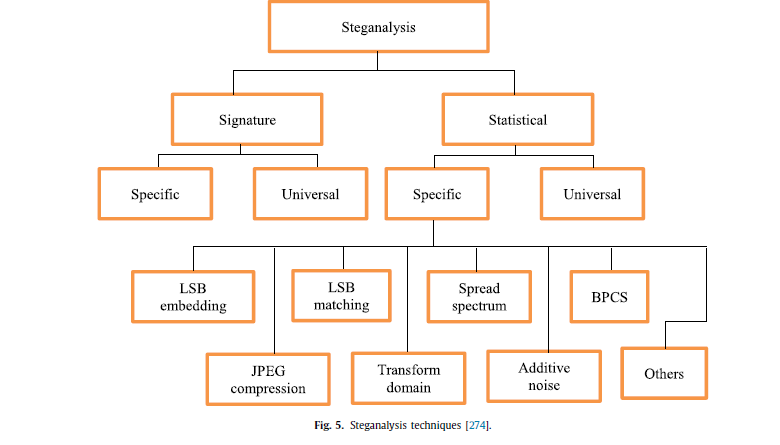
For evaluating the different aspects of image steganography, dif- ferent metrics are used [49,50] . Some of the popular metrics in- clude Peak Signal to Noise Ratio, Correlation coefficient, histogram comparison, Structured Similarity Index Measure (SSIM) and Pay- load Capacity.



Popular machine learning systems used in the steganographic area include, Sup- port Vector Machine (SVM) [231,232] , Decision-tree based analysis, Genetic Algorithm (GA) [233–237] , Fuzzy Logic (FL) optimization techniques [82,238–242] and Neural Networks (NN) [243–246] . All of these attempts make use of artificial intelligence techniques for pre-processing and/or for defining embedding nature and/or for limiting or extending the embedding stages or extracting process.

Cover image selection

In a steganographic process, the main concern is to embed a se- cret data in the cover media without leaving any suspicious noise in the embedded image. Thus, the embedding efficiency mainly de- pends on the nature of embedding processes and are explained in the previous sections. However, the efficiency also depends on the selected cover image. In this section, the discussion is about the significance of cover image in a steganographic process. As we detailed before, the embedding will be more detectable in the smooth regions in the image while it is difficult to find over the textured or edge regions. Hence, it can be stated that the cover image will possess high fidelity regions to make the embedding in an imperceptible way. This will also help to conceal more secret data bits without creating any visible noise in the stego-image. For selecting the appropriate cover image, a lot of methods were pro- posed and most of them select the ones with more frequency com- ponents rather than smooth regions [268,269] . Some of the earlier work uses correlation-based cover selection procedure, the simi- larity of image blocks [270] and over statistical measures features. Then, more image information is taken for the selection of a suit- able cover image from an available dataset. In the article [268] , a correlation-based cover image selection process is employed. The LSB bits of wavelet coefficients of the cover images are correlated with the secret data and the most matching cover image is se- lected from the dataset. Another approach of cover image selection is demonstrated in the paper [271] . A fuzzy based image complex- ity model is used to find a least detectable stego-image by check- ing the image dataset. Another cover image selection method is explained in the paper [272] . This scheme uses Fisher Informa- tion Matrix and Gaussian Mixture Model for measuring the em- bedding ability for comparison. The main drawback of previous works is time consumption. An improved version of cover selection was proposed by Hajduk and Levický[273] to solve the above flaw. Here, accelerated optional cover selection based on shortening vec- tor of a secret message is used. In all of the cover image selection methods, the ultimate aim is to use a suitable cover image for the intended application. This will help to improve all required prop- erties of a steganographic process especially when the stego-image is possibly analysed using a steganalysis tool in the communication channel.



**33.** Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment

2019,springer

a29

@article{shanthakumari2019dual,

title={Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment},

author={Shanthakumari, R and Malliga, S},

journal={S{\=a}dhan{\=a}},

volume={44},

number={5},

pages={1--12},

year={2019},

publisher={Springer}

}

**Abstract-** The architecture development of cloud computing technology is growing tremendously in recent

times, which leads to improvement of scalability, accessibility and cost reduction measures in the IT sectors of

all enterprises. In this service, the data storage without reviewing security policies and procedures is a challenging

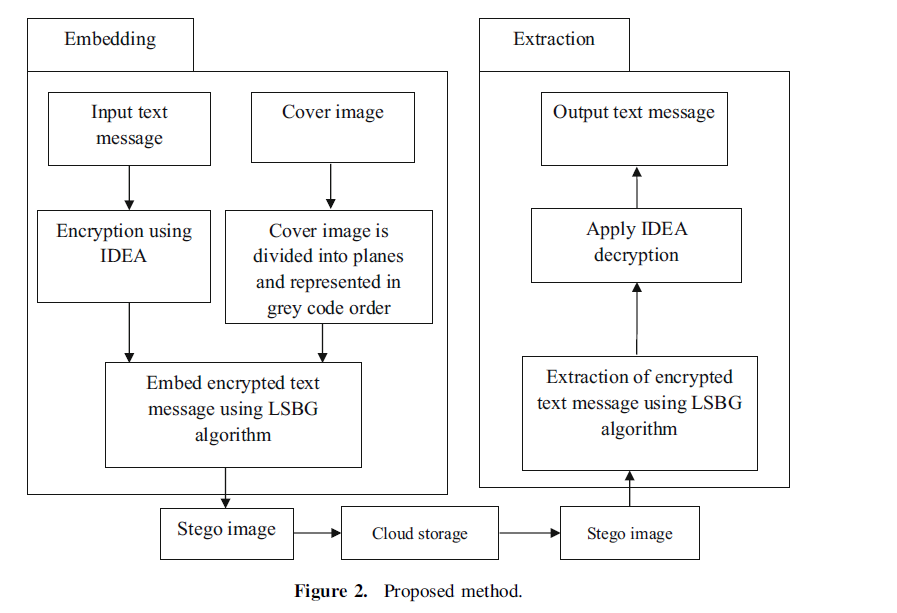
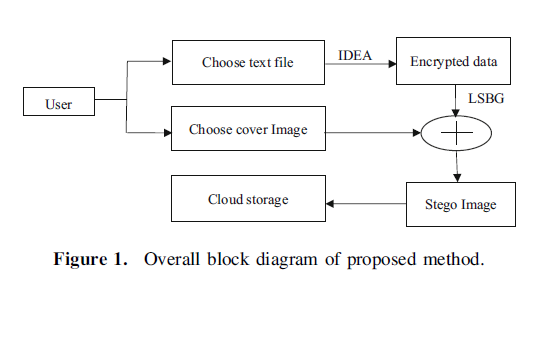
task and probabilities of extracting secret information by an unauthorized intervention are more.

However, to prevent the breaches of security in the cloud service, the steganography art plays an essential role in

the data communication medium to improve the security measures, and it is an indispensable technique for

hiding the secret information into a cover object. **This paper describes the implementation of new steganography method with International Data Encryption Standard Algorithm (IDEA) and Least Significant Bit Grouping (LSBG) algorithm for embedding the secret information into an original image and extracting the same.** The result shows the improvement of data embedding capacity and reduces the issues related to data security by effective utilization of this new approach, which reveals the remarkable achievement of the combinational execution of steganography and cryptography technique. The IDEA and LSBG have some vital qualities such as data confidentiality, integrity verification, capacity and robustness, which are crucial factors to achieve successful

implementation of steganography process in data security system. The effectiveness and properties of the stego image can be evaluated by some specific measures like mean squared error, root mean squared error, peak signal to noise ratio and structural similarity index matrix to analyse the image quality. The results show that the proposed technique outperforms the existing methodologies and resolves the data security problem in data transmission and storage system of cloud computing services.

**Contribution-** 

Cryptography explains the

execution of IDEA to encrypt the secret information in the

form of text/file to attain high-level security. Another one is

LSBG algorithm, and grey code procedure to hide

encrypted messages in image pixels to protect the secret

information within the cover medium that forms one more

single layer of security. Finally, the primary target of duallayer

protection is achieved through the combined techniques

in the data transmission field.

**Limitation-**  and future intention is to implement this

method in audio and video steganography.

**34.A Survey on Cloud Data Security using Image Steganography**

**a25**

**@article{albalawi2020survey,**

**title={A Survey on Cloud Data Security using Image Steganography},**

**author={Albalawi, Afrah and Hamza, Nermin},**

**journal={International Journal of Advanced Computer Science and Applications},**

**volume={11},**

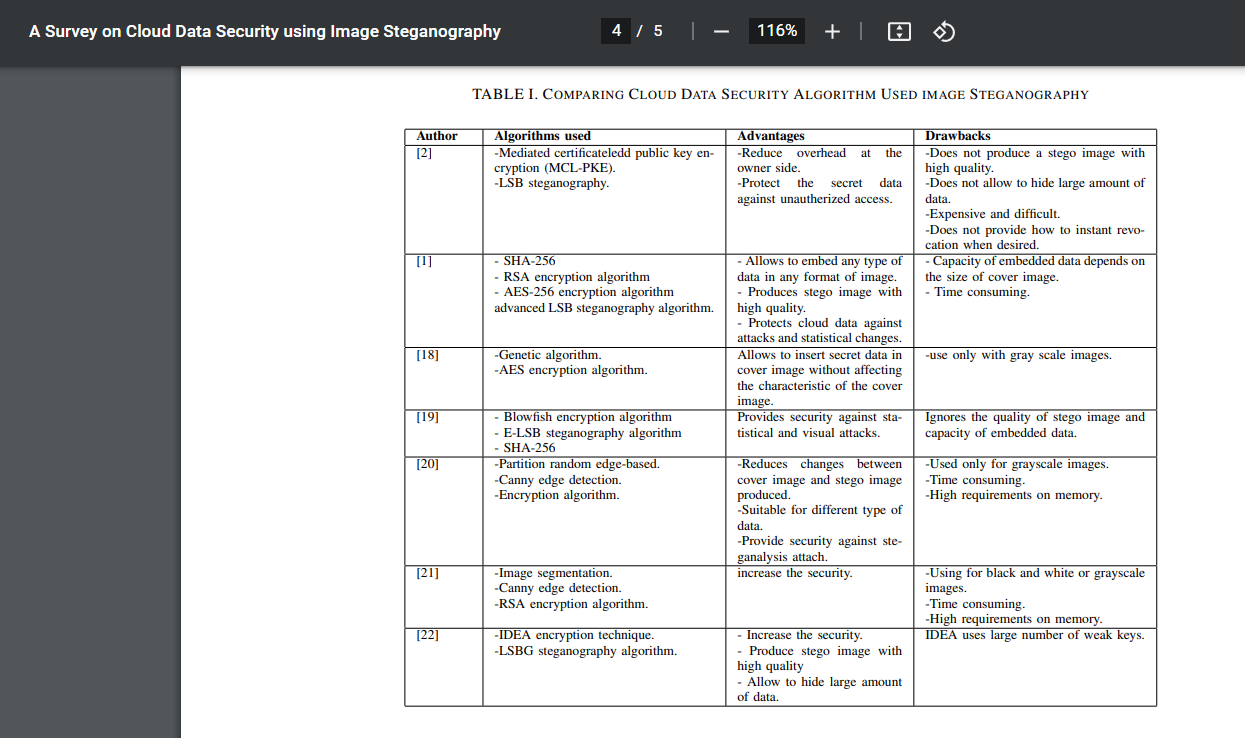
**number={1},**

**year={2020},**

**publisher={Science and Information (SAI) Organization Limited}**

**}**

**Abstract-** —Now-a-days, cloud computing proved its importance where it is being used by small and big organizations. The importance of cloud computing is due to the various services provided by the cloud. One of these services is storage as a service (SaaS) which allows users to store their data in the cloud databases. The drawback of this service is the security challenge since a third party manages the data. The users need to feel safe to store their data in the cloud. Consequently, we need for models that will enhance the data security. The image steganography is a way to protect data from unauthorized access. Image steganography allows users to conceal secret data in a cover image. In this paper, **we review and compare some of the recent works proposed to protect cloud data using image steganography.** The first comparison of models based on the algorithms they used, advantages and drawbacks. The second comparison of the models based on the aims of steganography: quality where the model produces a stego-image with high quality, security where the secret data is difficult to detect and capacity where the model allows to hide large amounts of data

**Contribution-** 

**35.A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage**

**springer,2020**

**A30**

**@article{sukumar2020secure,**

**title={A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage},**

**author={Sukumar, Arunkumar and Subramaniyaswamy, V and Vijayakumar, Varadarajan and Ravi, Logesh},**

**journal={Multimedia Tools and Applications},**

**volume={79},**

**number={15},**

**pages={10825--10849},**

**year={2020},**

**publisher={Springer}**

**}**

**Abstract-** Cloud computing is widely accepted by both individuals and enterprises alike for the

storage of multimedia contents. It is due to the introduction of a new architecture where the

cost of computation, storage, and services needed for maintenance for storage of multimedia

are less. Cloud computing addresses the scarcity of resources for clients by offering

options to pay for services only as they are used. But once the organization’s multimedia

contents are uploaded into cloud space, the user loses control over their contents which

may no longer be safe. The cloud user has to take some measure to avoid privacy issues.

Steganography is preferred over encryption for providing multimedia security as content

concealed in a cover image is not revealed. **The multimedia content is transformed using**

**Discrete Rajan Transform (DRT) and embedded into a chosen cover image which is**

**created by IntegerWavelet using Diamond Encoding Scheme**. Generated stego images are

stored in the cloud. When the multimedia content is required, stego images are

downloaded from the cloud and are subjected to inverse transform of IWT. **SVMprovides**

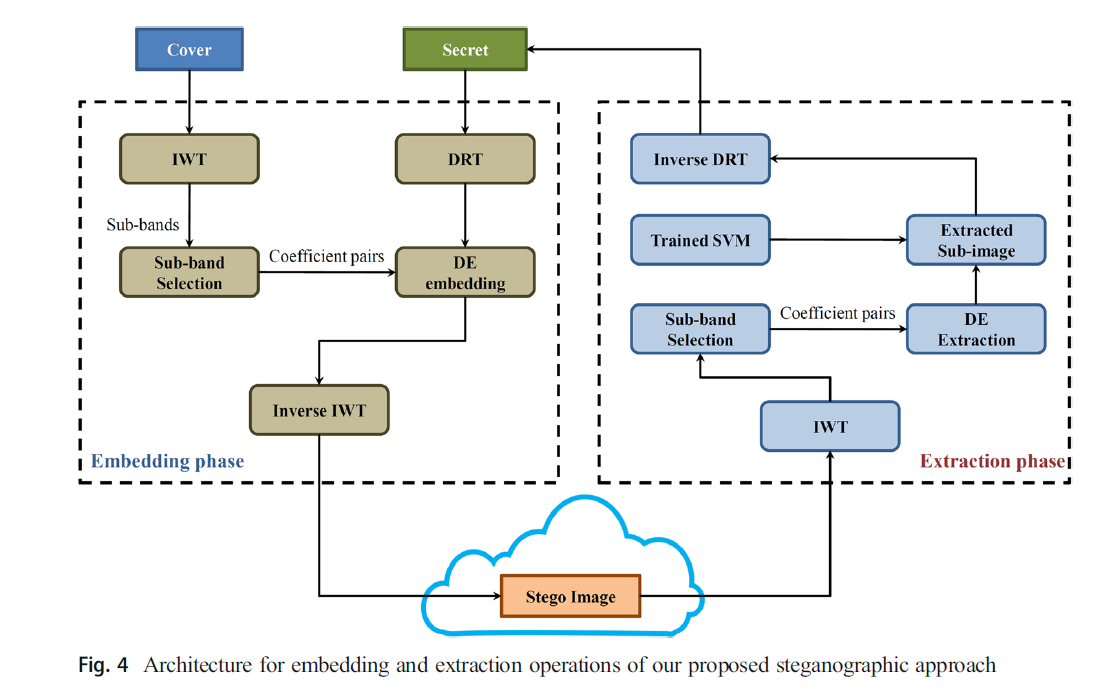
**Good learning ability to our extraction process which makes our algorithm more robust to**

**various attack**s, viz., salt and pepper noise, Gaussian noise, cropping, compression, etc.

Experimental values for Peak Signal to Noise Ratio (PSNR) for two secret images are 53

and 50 respectively which is better over the available schemes in the literature. Similarly

for robustness and security evaluation, our scheme provides a better result.

**Contribution-** 

Salient features of our approach

The proposed steganographic scheme is an enhanced variant of the existing approach by

following aspects:

1. The secret image is transformed using a Discrete Rajan Transform (DRT) before embedding.

DRT is used to increase the security of the secret image. DRT performs many rounds

of shifting and does some mathematical operations on the secret image. So steganalysis

cannot be done based on pattern matching or using any other image processing techniques.

2. DRT transformed images are subjected to Base b (b = 2 k 2 + 2 k + 1, where k ≥ 1 is

embedding parameter) conversion. It increases the embedding rate to some extent.

3. In DWT, integer pixel values of the secret image are converted into double values while

transforming. While the inverse of DWT is applied, this double value may not be mapped

into an exact integer value. Because of wrong mapping, some amount of round of error is

introduced in the stego image. To overcome the roundoff error, IntegerWavelet Transform

is used for transformation.

4. SVM classifier is introduced in the extraction phase which increases the probability of

recovering the original secret image even after some image processing attacks are done on

the stego images.

**Limitation-**  In the future, we plan to enhance our work with a colour image steganographic technique for cloud storage.

**36.A Comprehensive Review on Image Encryption Techniques**

**Springer,2020**

**A18**

**Changes: a18-a19,a19-a20**

**@article{kaur2020comprehensive,**

**title={A comprehensive review on image encryption techniques},**

**author={Kaur, Manjit and Kumar, Vijay},**

**journal={Archives of Computational Methods in Engineering},**

**volume={27},**

**number={1},**

**pages={15--43},**

**year={2020},**

**publisher={Springer}**

**}**

**Abstract-** Image encryption techniques play a significant role in multimedia applications to secure and authenticate digital images.

This paper presents a comprehensive study of various image encryption techniques. This paper covers the most significant

developments in meta-heuristic based image encryption techniques. The various attacks and performance measures related

to image encryption techniques have also been studied. The existing techniques are analyzed with respect to differential,

statistical, and key analyses. **The main goal of this paper is to give a broad perspective on characteristics of image**

**encryption techniques.** The paper concludes by discussing significant advancements in the field of image encryption and

highlighting future challenges.

**Contribution-** 

37.Towards DNA based data security in the cloud computing environment

2020,elsevier

**Abstract-** Nowadays, data size is increasing day by day from gigabytes to terabytes or even petabytes, mainly because of

the evolution of a large amount of real-time data. Most of the big data is transmitted through the internet and

they are stored on the cloud computing environment. As cloud computing provides internet-based services,

there are many attackers and malicious users. They always try to access user’s confidential big data without

having the access right. Sometimes, they replace the original data by any fake data. Therefore, big data security

has become a significant concern recently. Deoxyribonucleic Acid (DNA) computing is an advanced emerged

field for improving data security, which is based on the biological concept of DNA. **A novel DNA based data encryption scheme has been proposed in this paper for the cloud computing environment.** Here, a 1024-bit secret key is generated based on DNA computing, user’s attributes and Media Access Control (MAC) address of the user, and decimal encoding rule, American Standard Code for Information Interchange (ASCII) value, DNA bases and complementary rule are used to generate the secret key that enables the system to protect against many security attacks. Experimental results, as well as theoretical analyses, show the efficiency and effectivity of the proposed scheme over some well-known existing schemes.

**Contribution-** 

**Limitation-**

**38.Hybrid Design for Cloud Data Security Using Combination of AES, ECC and LSB-Steganography**

**A31**

@article{hosam2019hybrid,

title={Hybrid design for cloud data security using combination of AES, ECC and LSB steganography.},

author={Hosam, Osama and Ahmad, Muhammad Hammad},

journal={Int. J. Comput. Sci. Eng.},

volume={19},

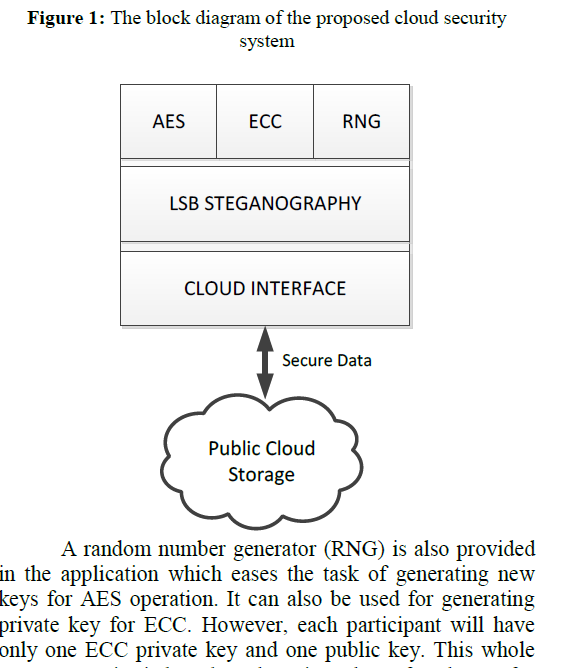
number={2},

pages={153--161},

year={2019}

}

**Abstract-** The ever-growing popularity of cloud systems is embarking a revolutionary change in information technology field. Parallel and flexible services offered by cloud technology are making it the ultimate solution for individuals as well as for organizations of all size. The grave security concerns present in cloud must be addressed to protect the data and privacy of huge number of cloud users. We present a hybrid solution to **tackle the key management problem**. **The data in the cloud is encrypted with AES encryption with private key. The AES 256-bits key is then encrypted with ECC. The ECC encrypted key will be embedded in the user’s image with LSB steganography**. If the user decided to share cloud data with a second user, he only need to embed the AES key in the second user’s image. Using Steganography, ECC and AES we can achieve strong security posture and efficient key management and distribution for multiple user

**Contribution-** 

**Limitation-**

**39.A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography**

**2022,mdpi**

**a8**

**@article{adee2022dynamic,**

**title={A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography},**

**author={Adee, Rose and Mouratidis, Haralambos},**

**journal={Sensors},**

**volume={22},**

**number={3},**

**pages={1109},**

**year={2022},**

**publisher={MDPI}**

**}**

**Abstract-** Cloud computing is a rapidly expanding field. It allows users to access computer system

resources as needed, particularly data storage and computational power, without managing them

directly. This paper aims to create a data security model based on cryptography and steganography

for data in cloud computing that seeks to reduce existing security and privacy concerns, such as data

loss, data manipulation, and data theft. To identify the problem and determine its core cause, we

studied various literature on existing cloud computing security models. This study utilizes design

science research methodology. The design science research approach includes problem identification, requirements elicitation, artifact design and development, demonstration, and assessment. Design thinking and the Python programming language are used to build the artifact, and discussion about its working is represented using histograms, tables, and algorithms. **This paper’s output is a fourstep data security model based on Rivest–Shamir–Adleman, Advanced Encryption Standard, and identity-based encryption algorithms alongside Least Significant Bit steganography. The four steps are data protection and security through encryption algorithms, steganography, data backup and recovery, and data sharing.** This proposed approach ensures more cloud data redundancy, flexibility, efficiency, and security by protecting data confidentiality, privacy, and integrity from attackers.

**Contribution-** To

protect cloud data, we introduced a dynamic four-step model with hybrid encryption,

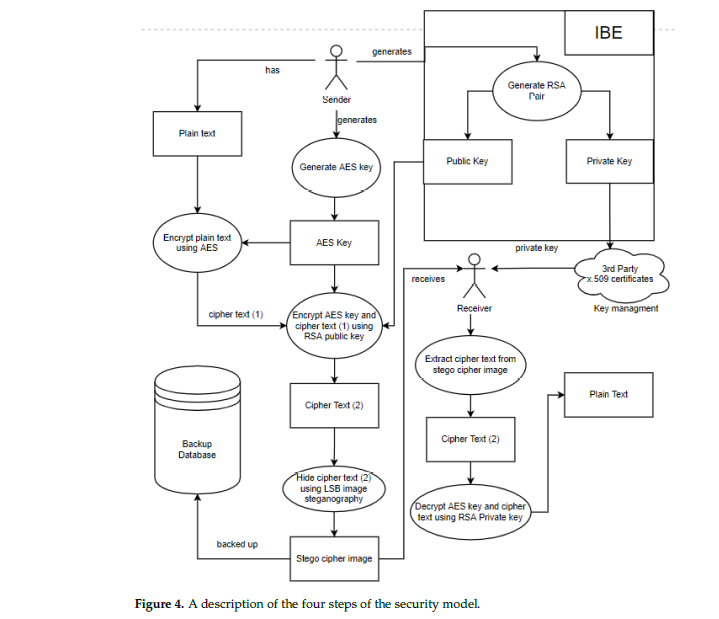
in which the AES-256 symmetric method is paired with the RSA asymmetric technique.

The encrypted data are then concealed in a photo using the LSB steganography technique.

The users’ chosen strategies can be used to back up the results of the decryption process.

With identity-based encryption (IBE), the results of the encryption and decryption may be

shared and securely transferred to authorised recipients.



**Limitation-**

40.**Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography**

**A9**

2020,ieee

@inproceedings{abbas2020security,

title={Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography},

author={Abbas, Mustafa S and Mahdi, Suadad S and Hussien, Shahad A},

booktitle={2020 International Conference on Computer Science and Software Engineering (CSASE)},

pages={123--127},

year={2020},

organization={IEEE}

}

**Abstract-** One of the significant advancements in information

technology is Cloud computing, but the security issue of data

storage is a big problem in the cloud environment. That is why a

system is proposed in this paper for improving the security of

cloud data using encryption, information concealment, and

hashing functions. **In the data encryption phase, we implemented**

**hybrid encryption using the algorithm of AES symmetric**

**encryption and the algorithm of RSA asymmetric encryption.**

**Next, the encrypted data will be hidden in an image using LSB**

**algorithm. In the data validation phase, we use the SHA hashing**

**algorithm. Also, in our suggestion, we compress the data using**

**the LZW algorithm before hiding it in the image.** Thus, it allows

hiding as much data as possible. By using information

concealment technology and mixed encryption, we can achieve

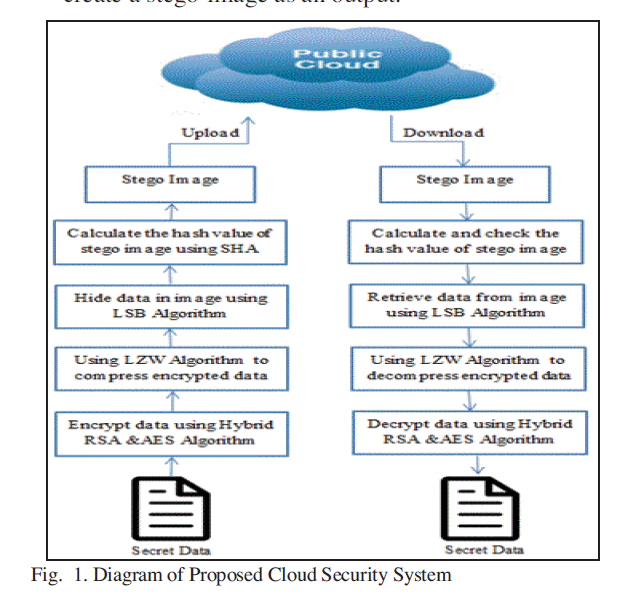
strong data security. In this paper, PSNR and SSIM values were

calculated in addition to the graph to evaluate the image masking

performance before and after applying the compression process.

The results showed that PSNR values of stego-image are better

for compressed data compared to data before compression.

**Contribution-** 

**41.A New Fuzzy-DNA Image Encryption and Steganography Technique**

**a32**

**@article{el2020new,**

**title={A new fuzzy-DNA image encryption and steganography technique},**

**author={El-Khamy, Said E and Korany, Noha O and Mohamed, Amira G},**

**journal={IEEE Access},**

**volume={8},**

**pages={148935--148951},**

**year={2020},**

**publisher={IEEE}**

**}**

**Abstract-** Image encryption and steganography techniques are receiving a lot of interest and investigations due to their high importance in multimedia communication systems. A novel highly efficient image encryption and steganography technique are presented in this paper. **For the first time, the proposed technique uses hybrid DNA encoding and Choquet’s Fuzzy Integral sequence**s. At first, a confused version of the image, using a simple chaotic map, is encoded using DNA’s bases. Four coded images are generated using the four DNA bases, namely AT, CG, GC, and TA. Parallel to that, a Choquet’s fuzzy Integral sequence is generated and DNA encoded similarly to obtain four pseudo-random sequences. Secondly, the resulting four fuzzy/DNA sequences are used to diffuse the four DNA encoded images using the complementary DNA XOR rule, according to certain control code. Finally, the wavelet fusion algorithm is then used to

fuse the resulting four fuzzy-DNA encoded images, to get the encrypted image. For added security, a new steganography approach is used. In particular, the encrypted image is divided into four sub-images, each of which is hidden in a different carrier image selected from a known group of carrier images according to a given key. The simulation results and security analysis confirmed the efficiency of the proposed image encryption algorithm as well as the steganography approach used for enhanced security. Ten different images with a size of 256 ×256 are used to test the proposed method. The results show that the proposed algorithm has a higher key sensitivity. The pixel correlation coefficient values are very small (between 5.3220e-04 and

0.0011 horizontally, between 8.7670e-04 and 0.0022 vertically and between 0.0002 and 0.0045 diagonally).

Furthermore, the measured information entropy of the encrypted images is between 7.9970 and 7.9979

which are very close to the ideal value of 8. Additionally, the measured unified average changing intensity

and number of pixels change rate values take the values between 33.46 and 33.39 and between 99.61 and

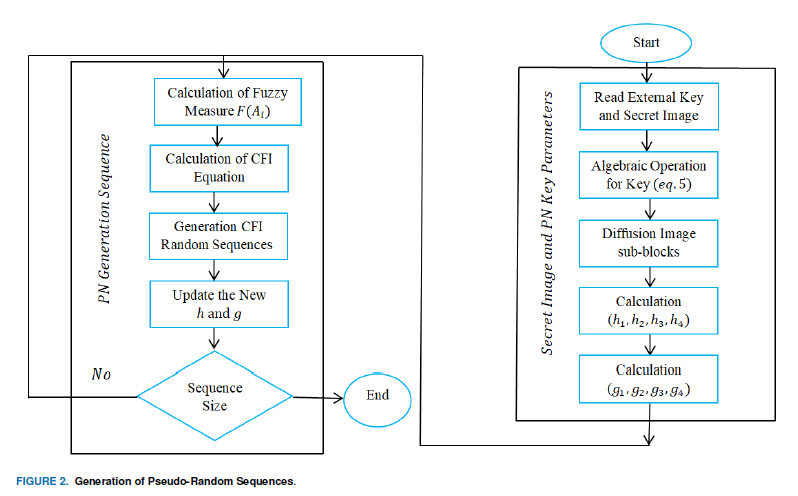
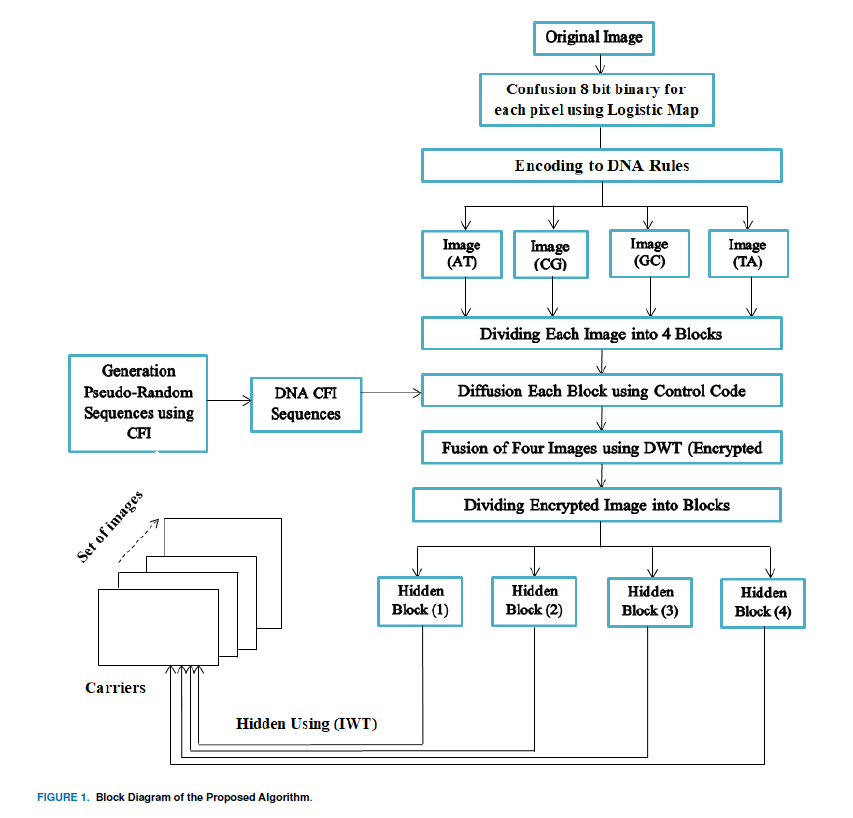
99.64, respectively, which are again closed to the ideal values. The steganography test shows that the hidden

encrypted images are almost invisible at high values of SNR and are characterized by good NCC values

under different types of attacks. The performance of the new proposed algorithm is proved to overcomes

many other previously published image encryption techniques.

**Contribution-**



**Limitation-**

**42.Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography**

**a33**

**@article{pandey2020secure,**

**title={Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography},**

**author={Pandey, Hari Mohan},**

**journal={Future Generation Computer Systems},**

**volume={111},**

**pages={213--225},**

**year={2020},**

**publisher={Elsevier}**

**}**

**Abstract-** This paper presents a bit mask oriented genetic algorithm based secure medical data transmission mechanism. A **bit mask oriented genetic algorithm (BMOGA) is utilized to reduce the replication of medical tests data which are transferred across organizations**. Medical data is considered very sensitive, therefore secure medical data transmission is must. BMOGA is a variant of the traditional genetic algorithm. Literature reveals that it can avoid premature convergence – a situation when optimization algorithms get stuck at local optimum. BOMGA utilizes Boolean based mask-fill operators and performs reproduction operations in two different phases that helps to avoid premature convergence.

Cryptographic features are integrated with the BMOGA for secure data transmission. The encrypted

data is embedded into the medical images through 1-level and 2-level Discrete Wavelet Transform

(DWT). The reverse process of the BMOGA is implemented for the extraction of secret message

from the encrypted one. Numerical experiments are conducted to determine the performance of the

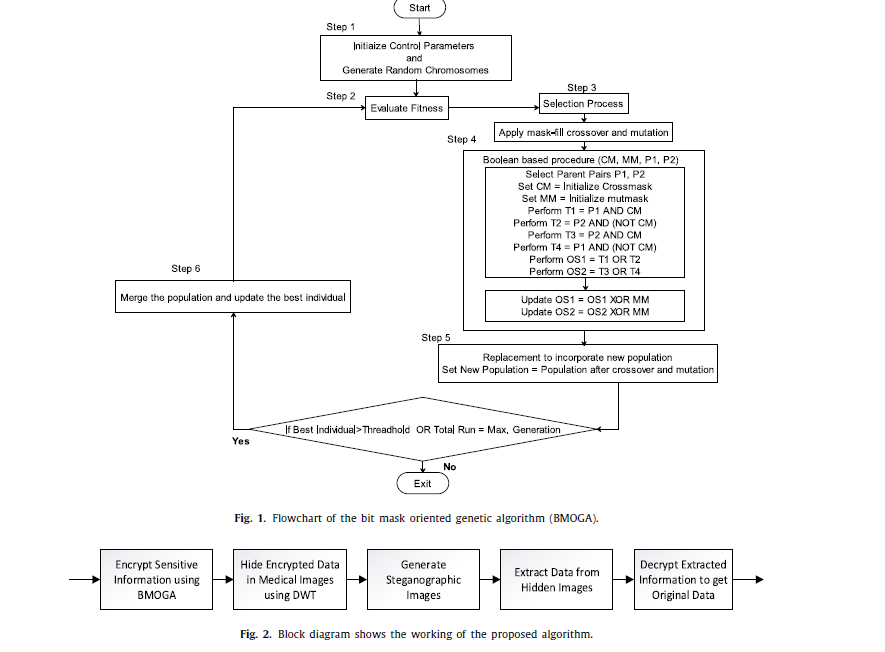
proposed algorithm. Results reveals that the proposed algorithm is capable of secure data transmission.

Performance comparison is done with the state-of-the-art algorithm with respect to the datasets.

Comparative results indicated the superiority of the proposed algorithm in terms of various statistical

measures such as peak signal to noise ratio (PSNR), correlation, structural content (SC), structure

similarity (SSIM) and mean square error (MSE) to report the results.

**Contribution-** 

**Limitation-**

**43.**[**Encryption** and **Steganography** a secret **data** using circle shapes in colored images](https://iopscience.iop.org/article/10.1088/1742-6596/1591/1/012019/meta)

a10

**@inproceedings{al2020encryption,**

**title={Encryption and Steganography a secret data using circle shapes in colored images},**

**author={Al-Kateeb, Zeena N and Al-Shamdeen, Muna Jaffer and Al-Mukhtar, Farah Saad},**

**booktitle={Journal of Physics: Conference Series},**

**volume={1591},**

**number={1},**

**pages={012019},**

**year={2020},**

**organization={IOP Publishing}**

**}**

**Abstract-** Since the earliest times, people have used the encryption and hiding data to achieve a safe

and reliable transfer of important data. This paper propesed a new method for **encrypting important**

**data based on the circular shapes information that extracted from the cover image**, The encryption

process is done using an update of a well known traditional method with simple calculations taking

advantage of the coordinates of the center of the main circle as keys extracted from the cover image

to reduce the number of keys exchanged between the sender and the recipient and to increase the

level of security and confidentiality. The hiding process of the encrypted data is done **in pixels that**

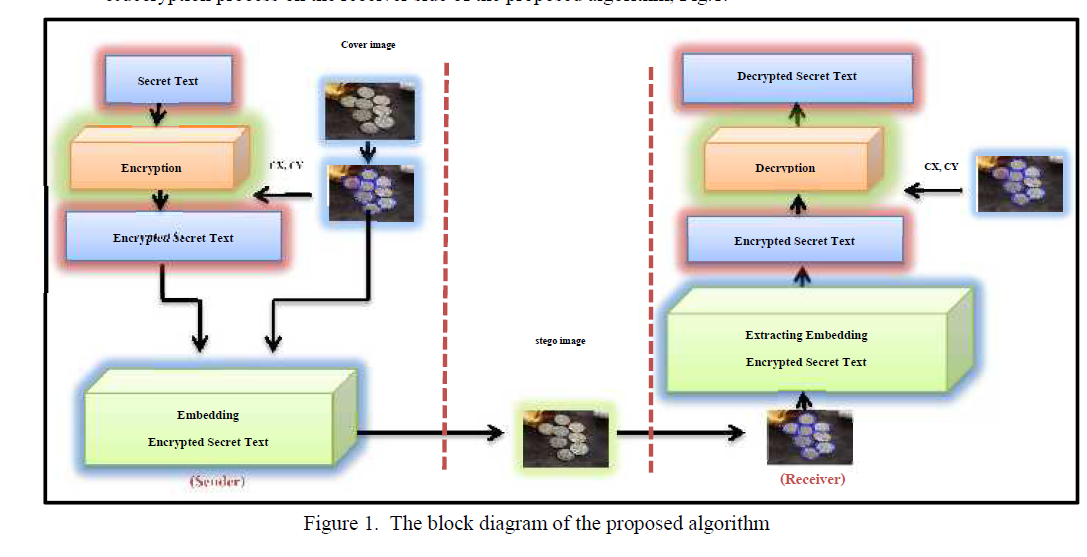
**located in the circular areas of the cover image and in three forms of concealment, which providing**

**second encryption, choosing the hiding form depending on the appearing sequence of the character in the text, which makes decode the secure data will be so difficult**, the experiments showed that the

proposed method was achieved excellent encryption and hiding depending on the coefficients Peak

Signal to Noise Ratio analyses (PNSR), Mean Square Error (MSE), and other measurements. The

proposed method achieves a complete data recovery ratio where it was Bit Error Rate BER=0

**Contribution-** Encryption The Secret Text Steps:

1. Enter the secret text, plain text (PT)

2. Choose the cover image (CovIm)

3. **Find circles in color images (CA)**

**4. Determine the center coordinates of main circle CX, CY, to use those coordinates in the**

**encryption process**

5. Encrypt the secret text using Caesar method based on the center coordinates of the main

circle such as the following:

• Cipher text1 (CT1) = (PT) + (CX)

• Cipher text 2 (CT2) = (CT1) - CY

6. Get encrypted text

7. Repeat step 5 until all plain text is encrypted

**3.2 Embedding The Encrypted Secret Text Steps:**

1. Enter the secret ciphertext (CT2)

2. Choose the cover image (CovIm)

3. **Find circles in the cover color image (CA)**

4. Store all coordinates of the points within the circular regions in N\*2 array lets ACP, where N is a

no. of points within the circular regions, ACP[i][1] contains the X-axis coordinates of i point

within the circular region, ACP[i][2] contain the Y-axis coordinates of i point within the

circular region

5. Convert a character of the secret ciphertext (CT2) to asci\_code (AsciCT2)

6. Convert the asci\_code for a character of the secret ciphertext (AsciCT2) to binary code

(BCT2)

7. Select a map to hide the character, depending on the location which that contain the character

based on the following:

If (ACP[i][1]\* ACP[i][2])%3

• =0 the hiding map a character is Blue Green Red (BGR)

• =1 the hiding map a character is Green Red Blue (GRB)

• =2 the hiding map a character is Red Green Blue (RGB)

9. Embedding a cipher character from secret ciphertext in a determined pixel of a cover image

10. Repeat step 5\_7 until all ciphertext characters are embedding

11. Get the stego image (StegoIm)

**44.Enhancing the security of cloud data using hybrid encryption algorithm**

a34

@article{sajay2019enhancing,

title={Enhancing the security of cloud data using hybrid encryption algorithm},

author={Sajay, KR and Babu, Suvanam Sasidhar and Vijayalakshmi, Yellepeddi},

journal={Journal of Ambient Intelligence and Humanized Computing},

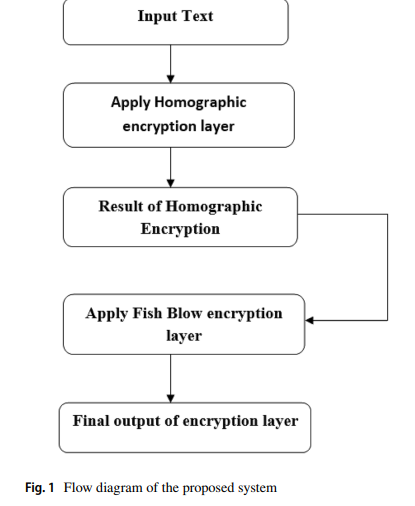
pages={1--10},

year={2019},

publisher={Springer}

}

**Abstract-** Cloud computing is a term which is employed to explain diferent concepts of computing that includes several PCs linked through a real time network of communication such as internet. Cloud computing is a developing paradigm which has in the recent times attracted lot of researchers because of its capability to decrease the costs related with computing. Due to the rapid growth of cloud computing techniques the rapid raise of services of cloud became outstanding. In today’s world data security is a challenging problem. The essential issue related with cloud computing is the security of cloud and the proper cloud implementation over the network. In cloud the models of security namely confdentiality, authentication, accessibility, data recovery and data integrity. It includes services of cloud, model of deployment, security problems and barriers in cloud computing. Nowadays, enhancing security of data in cloud has become a major concern and the solution for this is to apply appropriate encryption techniques while storing the data in the cloud. This study proposes a hybrid algorithm to enhance security of cloud data using encryption algorithm. The main purpose of using encryption algorithms is to secure or store huge amount of information in cloud. **This study combines homographic encryption and blowfsh encryption to enhance cloud security**. It can be concluded that if the security issues are resolved then the future will be the solutions for cloud storage for small as well as large frms.

**Contribution-** 

**Limitation-**

**45.Auto encryption algorithm for uploading data on cloud storage**

**a22**

**@article{tajammul2020auto,**

**title={Auto encryption algorithm for uploading data on cloud storage},**

**author={Tajammul, Mohd and Parveen, Rafat},**

**journal={International Journal of Information Technology},**

**volume={12},**

**number={3},**

**pages={831--837},**

**year={2020},**

**publisher={Springer}**

**}**

**Abstract-** Cloud computing is a scalable, reliable, and fast

growing technology. It offers a no. of services to the users

on pay per use basis. These services includes: computation,

storage, and various types of applications etc. It is spread

all over the world with its global and robust infrastructure.

This paper focuses on storage security of cloud computing.

It has been found in past few years that cloud storage is not

fully secured. It is in its early stage in terms of security and

privacy of users’ data. Various algorithms have been

designed and implemented so far, all of them seek to user

for creating and entering key to encrypt data rather than

generating key their self. **This research paper proposed an**

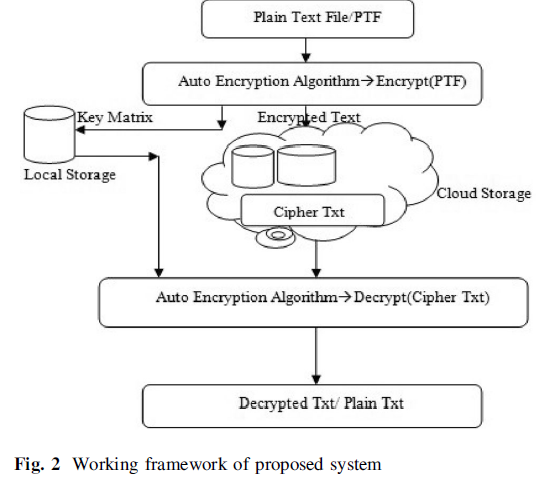
**algorithm which will produce key itself on the basis of data**

**input and subsequently encrypt data on the basis of key**

**produced.** Encrypted data will be uploaded on cloud storage

while key is kept secure at local server for future use to

decrypt the data.

**Contribution-** 

Results show that the Auto Encryption algorithm produces better results than that of AES algorithm.

46.[New fully homomorphic **encryption** scheme based on multistage partial homomorphic **encryption** applied in **cloud** computing](https://ieeexplore.ieee.org/abstract/document/8640952/)

A23

@inproceedings{mahmood2018new,

title={New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing},

author={Mahmood, Zainab Hikmat and Ibrahem, Mahmood Khalel},

booktitle={2018 1st Annual International Conference on Information and Sciences (AiCIS)},

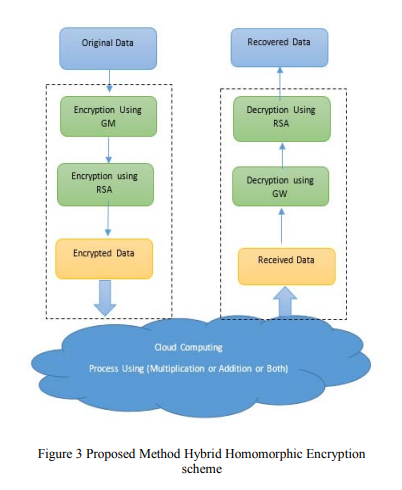
pages={182--186},

year={2018},

organization={IEEE}

}

**Abstract-** The paper presents an overview of security issues in cloud computing and utilization of the fully homomorphic encryption technique has drawbacks of large key size and low calculation efficiency, and it is not practical for the secure cloud computing. We build up a hybrid homomorphic encryption scheme based on the GM encryption algorithm which is additively (single bit) homomorphic, and RSA algorithm which is multiplicative homomorphic. The hybridization of homomorphic encryption schemes seems to be an effective way to defeat their limitations and to benefit from their resistance against the confidentiality attacks. This hybridization of homomorphic encryption algorithm lead to increase the speed (2.9) times, reduce the computation time to 66% percentage from previous one, enhanced confidentiality of the data that is stored in the cloud by enhancing security (two layer of encryption methods used) . Since hybrid encryption is utilized high security and authentication is provided.

**Contribution-** 

—-----------------------------------------------------------------------------------------------------------------------------------

**47.Image Encryption and Analysis using Dynamic AES**

@INPROCEEDINGS{8727711,

author={Singh, Amandeep and Agarwal, Praveen and Chand, Mehar},

booktitle={2019 5th International Conference on Optimization and Applications (ICOA)},

title={Image Encryption and Analysis using Dynamic AES},

year={2019},

volume={},

number={},

pages={1-6},

doi={10.1109/ICOA.2019.8727711}}

**Abstract: AES (Advanced Encryption Algorithm) is a block cipher, which is world wide implemented for encryption of data. It has been accepted as a standard for data security since 2001. AES is a substitution and permutation cipher, which provides confusion by using substitution box (S-Box) in the algorithm. The main drawback of AES is that it uses static S-Box throughout algorithm, which compromise the security of AES and may be exposed to different algebraic attacks. So to overcome this problem new Dynamic AES algorithm developed by key dependent dynamic S-Box using dynamic irreducible polynomial and affine constant. The analysis is done on gray scale and colour images. Both the images are encrypted and decrypted by using standard AES and Dynamic AES. Quality of algorithm and the level of security is analyzed based on the parameters like Image Histogram Analysis, Adjacent Pixel Correlation Analysis, Image Entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Encryption Quality. Index Terms—AES, Dynamic AES, NPCR, UACI, Encryption Quality, Image Entropy**

48.A novel hybrid permutation substitution base colored image encryption scheme for multimedia data

<https://www.sciencedirect.com/science/article/abs/pii/S221421262100065X>

@article{naseer2021novel,

title={A novel hybrid permutation substitution base colored image encryption scheme for multimedia data},

author={Naseer, Yasir and Shah, Tariq and Shah, Dawood},

journal={Journal of Information Security and Applications},

volume={59},

pages={102829},

year={2021},

publisher={Elsevier}

}

## Abstract

A novel hybrid permutation substitution-based color [image encryption](https://www.sciencedirect.com/topics/computer-science/image-encryption) scheme is presented. The permutation is [desirable property](https://www.sciencedirect.com/topics/computer-science/desirable-property) to have which make any security system diffusing. In present article, permutation is applied through p-box. The substitution process is also vital because it create confusion. In presented work substitution is applied through S-p-box. 3D mixed [chaotic map](https://www.sciencedirect.com/topics/computer-science/chaotic-map) is utilized to make our algorithm more diffusing and confusing. The permutation box, permutation substitution box and initial conditions of 3D mixed [chaotic map](https://www.sciencedirect.com/topics/computer-science/chaotic-map) are also utilized as a key. The experimental outcomes of proposed technique have been critically analyzed and a comprehensive comparison with existing schemes is presented.

49.Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions

@inproceedings{Liu2003SelectiveEO, title={Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions}, author={Xilin Liu and Ahmet M. Eskicioglu}, year={2003}, url={https://api.semanticscholar.org/CorpusID:16826546} }

ABSTRACT The security of multimedia data in digital distribution networks is commonly provided by encryption, i.e., the mathematical process that transforms a plaintext message into unintelligible ciphertext. Nevertheless, the classical and modern ciphers have all been developed for the simplest form of multimedia data, i.e., text, and are not appropriate for higher forms such as images and video with very large file sizes. Selective encryption is a recent approach to reduce the computational requirements for huge volumes of multimedia data in distribution networks with different client device capabilities. In this paper, we provide a survey and classification of the proposed schemes, discuss the current issues and present some future directions. Key words: Selective encryption, content protection, multimedia, cipher, JPEG, MPEG

**50.Multimedia Data Encryption based on Discrete Dyadic Transformation**

**@INPROCEEDINGS{8305898,**

**author={Prajwalasimha, S N and Surendra, Usha},**

**booktitle={2017 International Conference on Signal Processing and Communication (ICSPC)},**

**title={Multimedia data encryption based on discrete dyadic transformation},**

**year={2017},**

**volume={},**

**number={},**

**pages={492-495},**

**doi={10.1109/CSPC.2017.8305898}}**

Abstract²In this paper, confusion and diffusion based private key encryption algorithm is proposed. In the multimedia data neighboring pixels are strongly correlated with each other. The proposed encryption algorithm is the combination of both confusion and diffusion techniques. In the confusion algorithm, discrete dyadic transformation is used to shuffle the pixel positions and in the diffusion algorithm, modified Gingerbreadman sequence generator is used to alter the value of each pixel. The key length used is 128 bits. Each digit in the secret key is subjected for initial permutation and used along with diffusion algorithm for the key sequence generation. Keywords² Multimedia data; Public key encryption; Confusion; Diffusion; Discrete Dyadic Transformation; Gingerbreadman sequence generator

**51.High-Capacity Reversible Data Hiding for Encrypted Multimedia Data With Somewhat Homomorphic Encryption**

@ARTICLE{8491329,

author={Xiong, Lizhi and Dong, Danping and Xia, Zhihua and Chen, Xianyi},

journal={IEEE Access},

title={High-Capacity Reversible Data Hiding for Encrypted Multimedia Data With Somewhat Homomorphic Encryption},

year={2018},

volume={6},

number={},

pages={60635-60644},

doi={10.1109/ACCESS.2018.2876036}}

ABSTRACT This paper proposes a high-capacity reversible data hiding scheme for encrypted multimedia data by using Somewhat Homomorphic Encryption. In an image, three adjacent pixels are selected as a group for the whole process. In the encryption part, the original image is encrypted by an image provider. Then, the encrypted image is sent to data hider. In the data hiding part, two absolute differences can be obtained in each group. The additional data are embedded into the encrypted image by shifting histogram of the absolute differences. Moreover, a sorting technique that sorts the sum of two absolute differences in each group has good effects on reducing image distortion. The encryption and embedding operations are controlled by encryption and embedding/data hiding keys, respectively. If a receiver only has the data hiding key, the additional data can be extracted and the ciphertext can be restored. If the receiver has both the decryption key and the data hiding key, the additional data can be extracted and the original image can be restored. The experimental results have demonstrated the superiority of the proposed method over the existing similar methods.

**52.A Noval Method for Cloud Security and Privacy Using Homomorphic Encryption Based on Facial Key Templates**

@article{chandrasekhar2022noval,

title={A noval method for cloud security and privacy using homomorphic encryption based on facial key templates},

author={Chandrasekhar, Tadi and Kumar, Sumanth},

journal={Journal of Advances in Information Technology},

volume={13},

number={6},

year={2022}

}

Abstract—In the technology era, data is the key aspect, and securing the data is also an important task as many of the utilizers' presence online is on an incremental trend. There is a sustainable requirement to indulge the security procedures to secure the vulnerable data within cloud computing. In this regard, facial recognition is the latest technological trend in the field of biometrics and it is regarded as a fast processing technique that is available in computing devices as well as on mobile devices. The cloud computing services that include Microsoft, Google, and Amazon are utilizing different types of encryption techniques to include the aspect of privacy. The present method deploys a methodology that furnishes facial authentication and the generation of facial keys for the protection of data. The cloud mechanism is processed by facial features for authorization and authentication. The facial templates database is furnished for cloud encryption of each file that is integrated into the core algorithm of the method and the facial key is compared with the templates of the face data and later it is encrypted. The observed outcome of the study furnished a methodology that can guarantee that the information of the cloud user and the reclusive identification of the person is secured. In this study, the creation of a double abstraction methodology is performed to assure data protection on a cloud computing platform by utilizing facial templates as an important aspect of the process of encryption. The outcomes of the study show superior aspects to the state-of-art techniques. Index Terms—facial recognition, bio-metrics, securing, cloud mechanism, facial template, key features & CNN

53.**Improving cloud data security through hybrid verification technique based on biometrics and encryption system**

**@article{hossain2022improving,**

**title={Improving cloud data security through hybrid verification technique based on biometrics and encryption system},**

**author={Hossain, Md Alamgir and Al Hasan, Md Abdullah},**

**journal={International Journal of Computers and Applications},**

**volume={44},**

**number={5},**

**pages={455--464},**

**year={2022},**

**publisher={Taylor \& Francis}**

**}**

ABSTRACT Cloud computing is a unique network or environment where access, maintenance and process can be done from any part of the world. It is a customized internet-based computer server. It is a current trend of modern technology. For the massive computational power, it is the best option for storing data. There is no uncertainty that Cloud Data Server offers quick and solid types of assistance to its customers. When data is storing in the cloud storage the most important thing comes is the security of data. So, in recent years, cloud security is so much important issue because of the increasing of data. For the security of cloud computing, in this research, a hybrid verification technique is made which is based on biometric and encryption systems. In order to achieve strong and secure technique, this work use fingerprint as biometric technique and advanced encryption standard as a trustworthy encryption system. The primary goal of this paper is to avert information access from cloud information stockpiling focuses by unapproved clients. This new data security system can provide efficient authentication of cloud computing

54. Biometric-based cryptography for digital content protection without any key storage

@article{panchal2019biometric,

title={Biometric-based cryptography for digital content protection without any key storage},

author={Panchal, Gaurang and Samanta, Debasis and Barman, Subhas},

journal={Multimedia Tools and Applications},

volume={78},

pages={26979--27000},

year={2019},

publisher={Springer}

}

Abstract The traditional digital data security mechanisms follow either cryptography or authentication. The primary point of contention with these mechanisms remains either memorizing or securely storing the user’s credentials. The proposed work addresses this critical issue by presenting a fingerprint biometric-based mechanism to protect users’ digitized documents. In our approach, biometric features are extracted from the user’s fingerprint captured with a fingerprint biometric sensor. The extracted features are then used to generate a unique code utilizing the convolution coding principle. This unique code is further used to generate a cryptographic key for encryption and decryption of the user’s document. A sedulous investigation to our approach which includes experimentation with a variety of standard fingerprint images as the database starkly reveals a staggering 95.12 % true positive and 0 % as false negative. Further, the advantages of our approach are that it generates a unique key for each user and eliminates the storage of any biometric template or key. In addition, it is faster and accurate enough to develop any robust data storage security system.

55.**Biometrics for Internet-of-Things Security: A Review**

@article{yang2021biometrics,

title={Biometrics for internet-of-things security: A review},

author={Yang, Wencheng and Wang, Song and Sahri, Nor Masri and Karie, Nickson M and Ahmed, Mohiuddin and Valli, Craig},

journal={Sensors},

volume={21},

number={18},

pages={6163},

year={2021},

publisher={MDPI}

}

## **Abstract**

The large number of Internet-of-Things (IoT) devices that need interaction between smart devices and consumers makes security critical to an IoT environment. Biometrics offers an interesting window of opportunity to improve the usability and security of IoT and can play a significant role in securing a wide range of emerging IoT devices to address security challenges. The purpose of this review is to provide a comprehensive survey on the current biometrics research in IoT security, especially focusing on two important aspects, authentication and encryption. Regarding authentication, contemporary biometric-based authentication systems for IoT are discussed and classified based on different biometric traits and the number of biometric traits employed in the system. As for encryption, biometric-cryptographic systems, which integrate biometrics with cryptography and take advantage of both to provide enhanced security for IoT, are thoroughly reviewed and discussed. Moreover, challenges arising from applying biometrics to IoT and potential solutions are identified and analyzed. With an insight into the state-of-the-art research in biometrics for IoT security, this review paper helps advance the study in the field and assists researchers in gaining a good understanding of forward-looking issues and future research directions.

**Keywords:** [**biometrics**](https://www.mdpi.com/search?q=biometrics); [**IoT**](https://www.mdpi.com/search?q=IoT); [**security**](https://www.mdpi.com/search?q=security); [**access control**](https://www.mdpi.com/search?q=access+control); [**authentication**](https://www.mdpi.com/search?q=authentication); [**encryption**](https://www.mdpi.com/search?q=encryption)

56.**A Novel Key Generation Approach Based on Facial Image Features for Stream Cipher System**

@INPROCEEDINGS{9214095,

author={Sannidhan, M S and Sudeepa, K B and Martis, Jason E and Bhandary, Abhir},

booktitle={2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)},

title={A Novel Key Generation Approach Based on Facial Image Features for Stream Cipher System},

year={2020},

volume={},

number={},

pages={956-962},

doi={10.1109/ICSSIT48917.2020.9214095}}

Abstract—Security preservation is considered as one of the major concerns in this digital world, mainly for performing any online transactions. As the time progress, it witnesses an enormous amount of security threats and stealing different kind of digital information over the online network. In this regard, lots of cryptographic algorithms based on secret key generation techniques have been implemented to boost up the security aspect of network systems that preserve the confidentiality of digital information. Despite this, intelligent intruders are still able to crack the key generation technique, thus stealing the data. In this research article, we propose an innovative approach for generating a pseudo-pseudo-random key sequence that serves as a base for the encryption/decryption process. The key generation process is carried out by extracting the essential features from a facial image and based on the extracted features; a pseudo-random key sequence that acts as a primary entity for the efficient encryption/decryption process is generated. Experimental findings related to the pseudo-random key is validated through chi-square, runs up-down and performs a period of subsequence test. Outcomes of these have subsequently passed in achieving an ideal key.

57.**Multimedia Security Using Encryption: A Survey**

**@article{article,**

**author = {Hosny, Khalid and Ameen Zaki, Mohamed and Lashin, Nabil and Fouda, Mostafa and Hamza, Hanaa},**

**year = {2023},**

**month = {01},**

**pages = {1-1},**

**title = {Multimedia Security Using Encryption: A Survey},**

**volume = {PP},**

**journal = {IEEE Access},**

**doi = {10.1109/ACCESS.2023.3287858}**

**}**

Abstract:T Considering the current dependency on digital technology in modern society, the protection of multimedia is highly important. Encryption is vital in modern digital communication, ensuring data confidentiality, authentication, integrity, and non-repudiation. Multimedia encryption-based security techniques are becoming increasingly important as they allow for the secure sharing of multimedia content on digital platforms. This survey aims to review the state of secure and privacy-preserving encryption schemes applicable to digital multimedia, such as digital images, digital video, and digital audio. An extensive analysis of the existing cryptography schemes and multimedia encryption algorithms will be conducted to give an extensive overview of the current state of security encryption schemes specifically designed for digital multimedia technology. The survey results will be used to understand better the effectiveness and reliability of secure multimedia encryption schemes and contribute to developing efficient and secure encryption schemes in the future. INDEX TERMS Audio, encryption, image, multimedia, video

58.Lightweight Feistel structure based hybrid-crypto model for multimedia data security over uncertain cloud environment

@article{rayappan2021lightweight,

title={Lightweight Feistel structure based hybrid-crypto model for multimedia data security over uncertain cloud environment},

author={Rayappan, Denis and Pandiyan, Madhubala},

journal={Wireless Networks},

volume={27},

pages={981--999},

year={2021},

publisher={Springer}

}

Abstract The exponential rise in software computing and internet technologies have broadened the horizon of cloud computing applications serving numerous purposes like business processes, healthcare, finance, socialization, etc. In the last few years the increase is security breaches and unauthorized data access has forced industry to achieve computationally efficient and robust security system. The increase in multimedia data communication over different cloud applications too demands an efficient security model, which is expected to have low computational complexity, negligible quality-compromise and higher security robustness. Major conventional security-systems like cryptography and steganography undergo high computational overhead, thus limiting their potential towards cloud-communication where each data input used to be of large size and a gigantic amount of multimedia data is shared across the network. To alleviate above stated problems and enable a potential solution, in this paper a highly robust Lightweight Feistel Structure based Substitution Permutation Crypto Model is developed for multimedia data security over uncertain cloud environment. Our proposed model applies substitution permutation crypto concept with Feistel structure which performs substitution-permutation over five rounds to achieve higher confusion and diffusion. To retain higher security with low computation, we applied merely 64-bit block cipher and equal key-size. MATLAB based simulation revealed that the proposed lightweight security model achieves better attack-resilience even maintaining low entropy, high-correlation, and satisfactory computation time for multimedia data encryption. Such robustness enables our proposed security model to be applied for real-world cloud data security

59.**Biometric Security Through Visual Encryption for Fog Edge Computing**

**@ARTICLE{7898372,**

**author={Abdul, Wadood and Ali, Zulfiqar and Ghouzali, Sanaa and Alfawaz, Budour and Muhammad, Ghulam and Hossain, M. Shamim},**

**journal={IEEE Access},**

**title={Biometric Security Through Visual Encryption for Fog Edge Computing},**

**year={2017},**

**volume={5},**

**number={},**

**pages={5531-5538},**

**doi={10.1109/ACCESS.2017.2693438}}**

**ABSTRACT Fog and mobile edge computing have gained considerable attention from the research and development community. The problems related to security and privacy of biometric content are simpler to solve through edge computing resulting in improved security and privacy of biometric and other critically private information. Zero-watermarking has been proposed as a solution to help protect the ownership of multimedia content that is easy to copy and distribute. Visual cryptography is another approach to secure data that is to be shared through generating multiple shares. This paper is concerned with developing a biometric security solution for face images, using visual cryptography and zero-watermarking, that does not adversely impact the visual quality of the image. The original face image is not modified through the zerowatermarking and visual encryption procedures and this in turn does not adversely impact the recognition rate.**

60.**Securing Multimedia by Using DNA-Based Encryption in the Cloud Computing Environment**

@article{10.1145/3392665,

author = {Namasudra, Suyel and Chakraborty, Rupak and Majumder, Abhishek and Moparthi, Nageswara Rao},

title = {Securing Multimedia by Using DNA-Based Encryption in the Cloud Computing Environment},

year = {2020},

issue\_date = {October 2020},

publisher = {Association for Computing Machinery},

address = {New York, NY, USA},

volume = {16},

number = {3s},

issn = {1551-6857},

url = {https://doi.org/10.1145/3392665},

doi = {10.1145/3392665},

abstract = {Today, the size of a multimedia file is increasing day by day from gigabytes to terabytes or even petabytes, mainly because of the evolution of a large amount of real-time data. As most of the multimedia files are transmitted through the internet, hackers and attackers try to access the users’ personal and confidential data without any authorization. Thus, maintaining a strong security technique has become a significant concerned to protect the personal information. Deoxyribonucleic Acid (DNA) computing is an advanced field for improving security, which is based on the biological concept of DNA. A novel DNA-based encryption scheme is proposed in this article for protecting multimedia files in the cloud computing environment. Here, a 1024-bit secret key is generated based on DNA computing and the user's attributes and password to encrypt any multimedia file. To generate the secret key, the decimal encoding rule, American Standard Code for Information Interchange value, DNA reference key, and complementary rule are used, which enable the system to protect the multimedia file against many security attacks. Experimental results, as well as theoretical analyses, show the efficiency of the proposed scheme over some well-known existing schemes.},

journal = {ACM Trans. Multimedia Comput. Commun. Appl.},

month = {dec},

articleno = {99},

numpages = {19},

keywords = {CloudSim, American Standard Code for Information Interchange, decimal encoding rule, complementary rule, DNA computing, Cloud computing}

}

61.Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm

@article{shyla2022efficient,

title={Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm},

author={Shyla, S Immaculate and Sujatha, SS},

journal={Journal of Ambient Intelligence and Humanized Computing},

pages={1--13},

year={2022},

publisher={Springer}

}

Abstract Cloud computing is currently playing an important role in the information technology industry because of its improved efciency, wide access, low cost, and many benefts. It also provides more space for storing data and transmitting data from one location to another faster for diferent users on the Internet. Due to large storage, cloud customers can save huge capital investment on IT infrastructure and focus on their own core business. Therefore, many companies or organizations are moving their business to the cloud. However, many customers are reluctant to use the cloud due to security and privacy concerns. To tackle this problem, in this paper, efcient secure data retrieval is developed with the help of multi-stage authentication (MSA) and optimized blowfsh algorithm (OBA). The proposed system consists of three modules namely, MSA, data security, and data retrieval. Initially, the cloud users register their information on cloud based on a multi-authentication procedure. After the registration process, the data are encrypted with the help of OBA. To increase the security of the system, the key value is optimally selected with the help of a binary crow search algorithm. After the encryption process, MSA based data retrieval process is performed. This will avoid, un-authorized person to attack the data. The performance of the proposed methodology is implemented in JAVA and performances are analyzed in terms of diferent metrics.

62.**Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud**

@INPROCEEDINGS{8878749,

author={Sivakumar, P. and NandhaKumar, M. and Jayaraj, R. and Kumaran, A.Sakthi},

booktitle={2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)},

title={Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud},

year={2019},

volume={},

number={},

pages={1-5},

doi={10.1109/ICSCAN.2019.8878749}}

Abstract— Cloud security is a developing part of computer devices and network security. Cloud platform usage is for third-person information model. In Here we talk about how to provide protection for the information, from the illegal abuser and offer probity to the client. It requires an extremely high level of confidentiality and verification. One of the examples for cloud platform as a service is Heroku. The Heroku is based on a fully administered structure, which includes high data services and a great system, for implementing and operating current applications. The leading concern in cloud computing is data protection, so it can be used to handle the cryptographic methods. A probabilistic method to encrypt the information using AES. At AES algorithm is not only for protection it can be also used in huge speed. AES provides well-built security from third party. In this proposed work, we implemented Heroku is a cloud platform, and then we apply the AES method for data protection in Heroku cloud. AES cryptography is able to use for data security in cloud platform. And also using a dual cloud if one active or both active. If anyone cloud is active then the data should be more efficient in uploading and downloading operation perform in the cloud. Moreover, calculation delay in information to the encryption shows to better amount of information increase and the information time lag for encrypting information.

63.Enhancing the security of cloud data using hybrid encryption algorithm

@article{sajay2019enhancing,

title={Enhancing the security of cloud data using hybrid encryption algorithm},

author={Sajay, KR and Babu, Suvanam Sasidhar and Vijayalakshmi, Yellepeddi},

journal={Journal of Ambient Intelligence and Humanized Computing},

pages={1--10},

year={2019},

publisher={Springer}

}

Abstract Cloud computing is a term which is employed to explain diferent concepts of computing that includes several PCs linked through a real time network of communication such as internet. Cloud computing is a developing paradigm which has in the recent times attracted lot of researchers because of its capability to decrease the costs related with computing. Due to the rapid growth of cloud computing techniques the rapid raise of services of cloud became outstanding. In today’s world data security is a challenging problem. The essential issue related with cloud computing is the security of cloud and the proper cloud implementation over the network. In cloud the models of security namely confdentiality, authentication, accessibility, data recovery and data integrity. It includes services of cloud, model of deployment, security problems and barriers in cloud computing. Nowadays, enhancing security of data in cloud has become a major concern and the solution for this is to apply appropriate encryption techniques while storing the data in the cloud. This study proposes a hybrid algorithm to enhance security of cloud data using encryption algorithm. The main purpose of using encryption algorithms is to secure or store huge amount of information in cloud. This study combines homographic encryption and blowfsh encryption to enhance cloud security. It can be concluded that if the security issues are resolved then the future will be the solutions for cloud storage for small as well as large frms.

64.Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication

@article{faragallah2022cybersecurity,

title={Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication},

author={Faragallah, Osama S and El-Shafai, Walid and Sallam, Ahmed I and Elashry, Ibrahim and EL-Rabaie, El-Sayed M and Afifi, Ashraf and AlZain, Mohammed A and Al-Amri, Jehad F and El-Samie, Fathi E Abd and El-sayed, Hala S},

journal={Journal of Ambient Intelligence and Humanized Computing},

pages={1--25},

year={2022},

publisher={Springer}

}

Abstract Recently, the digital multimedia cybersecurity has become a research topic of interest due to the fast development of realtime multimedia applications over public networks such as the Internet. Therefore, this research paper introduces an efcient cybersecurity framework for protecting the high-efciency video coding (HEVC) frames. The suggested selective cybersecurity HEVC framework employs a robust hybrid technique based on watermarking and selective encryption for maintaining confdentiality and achieving copyright protection of the transmitted HEVC information. The watermarking method employs the Homomorphic transform and singular value decomposition in the discrete wavelet transform to increase the immunity of watermarked HEVC streams to attacks. Moreover, the selective encryption technique uses the Chaotic logistic map for encrypting the motion vector diference and the discrete cosine transform sign bits to provide the feature of HEVC format compliance with low encryption overhead cost. An extensive security investigation is carried out for the proposed selective HEVC cybersecurity framework. The obtained experimental outcomes ensure and validate the efectiveness of the selective HEVC cybersecurity framework for HEVC sequences transmission.

65.**Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification**

@ARTICLE{8630039,

author={Ge, Xinrui and Yu, Jia and Zhang, Hanlin and Hu, Chengyu and Li, Zengpeng and Qin, Zhan and Hao, Rong},

journal={IEEE Transactions on Dependable and Secure Computing},

title={Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification},

year={2021},

volume={18},

number={1},

pages={490-504},

doi={10.1109/TDSC.2019.2896258}}

Abstract—Verifiable Searchable Symmetric Encryption, as an important cloud security technique, allows users to retrieve the encrypted data from the cloud through keywords and verify the validity of the returned results. Dynamic update for cloud data is one of the most common and fundamental requirements for data owners in such schemes. To the best of our knowledge, the existing verifiable SSE schemes supporting data dynamic update are all based on asymmetric-key cryptography verification, which involves time-consuming operations. The overhead of verification may become a significant burden due to the sheer amount of cloud data. Therefore, how to achieve keyword search over dynamic encrypted cloud data with efficient verification is a critical unsolved problem. To address this problem, we explore achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification and propose a practical scheme in this paper. In order to support the efficient verification of dynamic data, we design a novel Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography to generate an authentication tag for each keyword. Benefiting from the accumulation property of our designed AAT, the authentication tag can be conveniently updated when dynamic operations on cloud data occur. In order to achieve efficient data update, we design a new secure index composed by a search table ST based on the orthogonal list and a verification list VL containing AATs. Owing to the connectivity and the flexibility of ST, the update efficiency can be significantly improved. The security analysis and the performance evaluation results show that the proposed scheme is secure and efficient.

66.**A Selective Video Encryption Scheme Based on Coding Characteristics**

@article{cheng2020selective,

title={A selective video encryption scheme based on coding characteristics},

author={Cheng, Shuli and Wang, Liejun and Ao, Naixiang and Han, Qingqing},

journal={Symmetry},

volume={12},

number={3},

pages={332},

year={2020},

publisher={MDPI}

}

## **Abstract**

The protection of video data has become a hot topic of research. Researchers have proposed a series of coding algorithms to ensure the safe and efficient transmission of video information. We propose an encryption scheme that can protect video information with higher security by combining the video coding algorithm with encryption algorithm. The H.264/AVC encoding algorithm encodes the video into multiple slices, and the slices are independent of each other. With this feature, we encrypt each slice while using the cipher feedback (CFB) mode of the advanced encryption standard (AES) with the dynamic key. The key is generated by the pseudo-random number generator (PRNG) and updated in real time. The encryption scheme goes through three phases: constructing plaintext, encrypting plaintext, and replacing the original bitstream. In our scheme, we encrypt the code stream after encoding, so it does not affect the coding efficiency. The purpose of the CFB mode while using the AES encryption algorithm is to maintain the exact same bit rate and produce a format compatible bitstream. This paper proposes a new four-dimensional (4-D) hyperchaotic algorithm to protect data privacy in order to further improve the security of video encryption. Symmetric encryption requires that the same key is used for encryption and decoding. In this paper, the symmetry method is used to protect the privacy of video data due to the large amount of video encrypted data. In the experiment, we evaluated the proposed algorithm while using different reference video sequences containing motion, texture, and objects.

**Keywords:** [**coding characteristics**](https://www.mdpi.com/search?q=coding+characteristics); [**semantic element**](https://www.mdpi.com/search?q=semantic+element); [**selective encryption**](https://www.mdpi.com/search?q=selective+encryption); [**hyperchaos**](https://www.mdpi.com/search?q=hyperchaos)

67.