Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture

DEBABRATA SAMANTA[1], **(Member, IEEE), AHMED H. ALAHMADI**[2], **KARTHIKEYAN M. P.**[3], **MOHAMMAD ZUBAIR KHAN**[2], **AMIT BANERJEE**[4], **GOUTAM KUMAR DALAPATI**[5], **AND SEERAM RAMAKRISHNA**[5], **(Senior Member, IEEE)**

[1]Department of Computer Science, CHRIST (Deemed to be) University, Bengaluru, Karnataka 560029, India
[2]Department of Computer Science and Information, Taibah University, Medina 42353, Saudi Arabia
[3]Department of Computer Science, PPG College of Arts and Science, Coimbatore 641035, India
[4]Physics Department, Bidhan Chandra College, Asansol, West Bengal 713303, India
[5]Center for Nanofibers and Nanotechnology, Department of Mechanical Engineering, National University of Singapore, Singapore 119260

Corresponding authors: Debabrata Samanta (debabrata.samanta369@gmail.com) and Mohammad Zubair Khan (mkhanb@taibahu.edu.sa)

ABSTRACT The growth of internet era leads to a major transformation in a storage of data and accessing the applications. One such new trend that promises the endurance is the Cloud computing. Computing resources offered by the Cloud includes the servers, networks, storage, and applications, all as services. With the advent of Cloud, a single application is delivered as a metered service to numerous users, via an Application Programming Interface (API) accessible over the network. The services offered via the Cloud are such as the infrastructure, software, platform, database and web services. The main motivation of this application model is to provide computationally secure key generation to protect the data via encryption. This key generation in the cryptography process falls into three categories in this research work. In the first part, *SVM* based encryption service model is constructed for which the key generation is from the conventional encryption operation mode with some improvements. To make the process more complex, the optimization techniques are taken into account for the key generation in descendant two methods application model that acts computationally more secure specifically for Cloud environment. The results of security analysis confirm the effectiveness of the proposed application model withstands potentially against various attacks such as Chosen Cipher Attack, Chosen Plain text Attack indistinguishable attacks for files. In case of images, it resists well against statistical and differential attacks. Comparative Analysis shows evidence of the efficiency of the developed pioneering application model quality and strength compared with that of the existing services.

INDEX TERMS Block chaining, cryptosystem, cloud computing, symmetric key, cryptography.

I. INTRODUCTION

A Computer Network is defined as a heterogeneous system, consisting of loosely coupled nodes and devices that share resources among one another through a data link. The communication and coordination between the nodes are handled by passing messages [12], [13]. The computer networks support numerous applications, storage, servers and transmit the data by means of diverse transmission mediums. The structure of a computer network consists of three main components, like the source and destination nodes, the medium through which the information is shared and finally an agreed communication protocols between the nodes for transmission. Conventional network models are categorized into two forms: Centralized and distributed. In the centralized model, a set of computers and devices are interconnected with one another and controlled by the master computer, through which the communication takes place [24]. In the scenario of distributed computing, loosely coupled systems are interconnected by a communication

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

network and have no centralized control. Advancement in modern internet skill permits hardware and software reserves as application Services, that can be delivered through Cloud based on the requirement. Cloud offers various services including software, infrastructure, platform, database etc. This shared pool of resources is offered as application services that can be accessed remotely besides the geographical locations [16]. The most interesting advantage of using Cloud services is that it offers resources on necessity as pay-as-you use metered services [45]. Its location-independent storage facilities, all the way through several cloud data centres, are another function of using cloud services. The Security-as a-Service that recommends the user to encrypt data through application models is one of the recent innovations in the Cloud computing paradigm. There is a lack of protection in existing Cloud Computing security models services that offers encryption as one source to the users. The file contains the sensitive information can encrypted when it is centralized into the servers or transferred over network to protect it from security related issues. Therefore, a new data security application model is introduced, that prevails over various security threats to the data transferred between communication medium by enabling encryption mechanisms [29]. High profiled encryption algorithm is applied to data for ease of access and authenticated access. Confidential information needs high authentication to protect it from unauthorized attacks. The multi-tenancy model and the pooled computing resources in computing have introduced new security challenges. Various security mechanisms like authentication, digital signatures, and cryptographic algorithms are used to protect data from unauthorized attacks. Achieving security with low cost computation is integral part of cryptography for both symmetric and asymmetric processes; key generation is the crucial step. Based on the efficiency of the key, the algorithm quality and strength will be defined. Various metrics such as the key length, number of keys, their mutual arrangement combinations provides better security. Authentication of the data is more important since it is shared among large number of users at same time [35]. Encryption mechanism defends the data from unauthorized access. The information shared may be a medical image or may be the patient health records as documents, or may be the spreadsheet files. In current era, images are widely used as a medium to share information over public networks in secured manner [22], [43]. Basically, the image encryption algorithms are divided into two, full encryption and partial encryption and works in blocks. The block ciphers are allowed to work on block of bits as well as bytes at a time for processing. The security-as-a-service offers an application model that encrypts different type of files converted to unintelligible [23]. Almost for all applications, the provider must guarantee their infrastructure is secure and data remains safe. Major issues like intrusions, modification or alteration of the data, hacking of data etc threatens the availability, authenticity, and confidentiality of the data will be resisted by utilizing this newly designed Cloud service model [5]. The Cipher
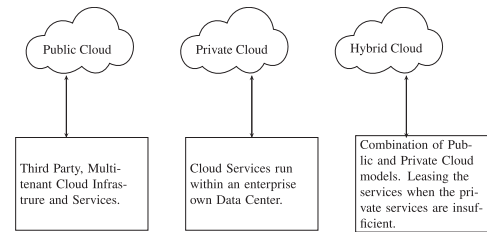

FIGURE 1. Cloud deployment models.

Block Chaining operation mode is the base for all the three new developed algorithms and focused much. Finally, varied tools used for the cryptanalysis are precisely stated in this work [25].

In present decade the distributed computing is widely used in many forms and seeks more attention towards security of the data being transferred. Network security standards and measures are enforced to protect both the data-in-transit and data-at-rest. The goal of security mechanisms is to resist the data from unauthorized accessing and attacks thwart hacking. The *NIST* (National Institute of Standards and Technology), Confidentiality assures that the information disclosed to unauthorized entities. Integrity assures that the intended data are changed by authorized entity only [31], [44]. Authenticity verifies the identity of entities is either valid or not. Authorization is the privilege that enable access to the resources by ensuring the individuality [1]. Figure 9 represents cloud deployment models.

A. NETWORK SECURITY CHALLENGE
There exist a lot of issues and challenges regarding the privacy of data being transferred through the open medium. Security mechanisms of the network are both captivating and difficult [17]. Before designing a security mechanism or an algorithm, the developer should concentrate on the prospective attacks on that security algorithm. Every algorithm is able to resist varied attacks based on its own properties and selection of intended algorithm based on the requirement is a major task to be competing by the developer [14]. Subsequently, continuous monitoring is essential to protect data from attacks [19]. General architecture diagram for cloud security is given in figure 2.

The attacks that jeopardize the network are broadly classified either as active or passive attack. An attack is said to be active if it is capable of altering the system resources or affecting its operations. The passive attack, are geared to gather information as opposed to gain the access to that information [41]. The attacks such as denial of service, breaking into the site, Data breach, resource usage, deception belong to active cadre while the sniffing, network traffic, sensitive information gathering belong to passive attacks cadre [39]. Data security is the vital goal of network security mechanisms. Data includes all forms such as the plain text file, Images in varied formats and sizes and multimedia files. The transmission of data through the communication channel without disclosure is the main task. In state of art, there
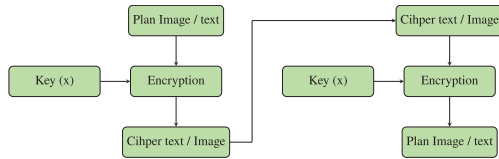
FIGURE 2. General architecture diagram for cloud security.

exists lot of security mechanisms such as Cryptography, Steganography, Access control Policies, Authentication mechanisms, Digital signature etc to avoid unauthorized threats and vulnerabilities. Among these protective measures, cryptography is the most widely used mechanism to protect data from intruders [4].

B. CRYPTOGRAPHIC ALGORITHMS

Mathematical algorithms are employed to change the user defined message (Plain text) into inarticulate format called as Cipher text. The art and science of protecting data using the mathematical algorithms are named as Cryptography. The cryptography is broadly classified into two categories based on the key such as the Symmetric Key Cryptography and Asymmetric Key Cryptography. Symmetric algorithms are traditional algorithms in which a single key is employed for both encipher and decipher process. Asymmetric key algorithms use public key for the encryption and private key for the decryption [25].

The cryptographic process has three dimensions: the type of operation performed to convert the plain text, the total number of keys used by the algorithm and the way in which the data is processed. The data processing is again classified either as blocks or as streams. Various cryptanalytic attacks in current scenario are cipher text only, known plain text, chosen plain text, chosen cipher text, chosen text, brute force, dictionary attack etc. The cryptographic algorithms offer various degrees of security to the data in the network. The potential of an algorithm depends on how well it resists against attacks and its complexity to compute. In decreasing order of the severity, there are four ways to hack the data such as a total break, global deduction, local deduction and information deduction [34]. Different components for cloud security are represented in [2, Fig.3]. Security algorithm falls into two types: an algorithm is said to be computationally weak or computationally strong. The computationally weak cryptographic algorithm allows the intruder to know some part of cipher data but cannot break the data with existing resources. In the scenario of the computationally strong algorithm, the intruder has less degree of familiarity with the cipher data. The ultimate goal of the cryptographic process is to protect data from disclosure by enforcing strong algorithms to defend the threats and vulnerabilities [33].

C. CLOUD COMPUTING

Cloud computing, a form of distributed computing, in which the user can access application at any time despite of place of access, by their linked services. It is the technology that
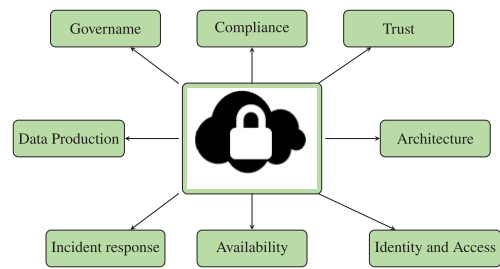

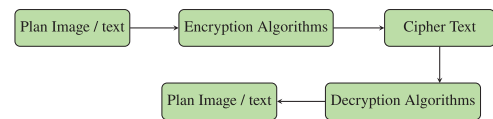**FIGURE 3. General architecture diagram for cloud security.**

FIGURE 4. Symmetric Cryptosystem.

contains a shared pool of resources, offered to the users, on-demand as metered service. In cloud computing, every resource is provided as services. The cloud computing is basically evolved from the grid, utility computing services and applications subscribed through the networks [15], [32]. Cloud offers services through the cloud application models. These models can be categorized as public cloud, private cloud, community cloud and hybrid cloud. The cloud computing architecture consists of two identical sections in which one is for the client interaction and another is for the cloud service providers [8].

The main objective of this proposed work is to provide an interesting application model offered as cloud service for data protection. This application model is designed in such a way to resist vulnerabilities and threats that jeopardize the data being transferred through an open communication medium. This could be possible with the strong cryptographic schemes with strong key generation mechanism. The application service, constructed in this research work consists of three different cryptographic algorithms with optimized key generations. A web service is built by combining these cryptographic processes and deployed in cloud as a service to encrypt assorted data types.

The reminder of this work is organized as follows. Section II, previous block chaining concept security and its related work, Section III discussed to proposed system Mechanism with an key Strategy, section IV presents proposed encryption Mechanism and existing systems experimental results comparison. Finally, section fifth provides the concluding remarks and future scope of the work.

II. LITERATURE REVIEW

Security is the process of protecting an object from unauthorized access. This security may be a physical state security else the theoretical state security. Protecting the messages or the data found in the network against various risks requires constant monitoring. The risk is defined as the collection

TABLE 1. List of active and passive attacks explained in [17].

Active Attacks	Passive Attacks
Intelligence Gathering	Information gathering
Breaking the site and steal the information	Passwords Hacking
Denial of Service	Sniffing the packets
Deception	Network Traffic
Resource Usage	Sensitive information modification

TABLE 2. Service offered by the security mechanisms result in Ali Dorri Salil S (2017) [10].

Security Mechanism	Services Offered
Cryptography	Confidentiality
Digital Signature Verification and Digital Certificates	Authentication
Identity Management	Integrity
Message Digest and Digital Signature	Non-Repudiation
Hash Technique, Encryption and Digital Signatures	Non-replay

TABLE 3. List of some symmetric key algorithms.

Algorithm	Length of the Key (in Bits)
Triple Data Encryption Standard(3DES)	64/112/168
Advanced Encryption Standard(AES)	128/192/256
IDEA	64/128
Blowfish	32-448
CAST-128	32/128
RC4	40/256
RC5	32/64/128

TABLE 4. Attack types attempted over the encrypted message.

Attack Type	Possibilities known to the Cryptanalyst
Known Plaintext	1. Algorithm processed for the encryption of data 2. The cipher text retrieved 3. Pairs of plain text and cipher text along with secret key
Chosen Plain text	1. Algorithm processed for the encryption of data 2. The cipher text retrieved 3. Plain text together with the subsequent cipher text and key is chosen by the cryptanalysts.
Chosen Cipher text	1. Algorithm processed for the encryption of data 2. The cipher text retrieved 3. Cipher text together with subsequent plain text and key chosen by the cryptanalysts.
Chosen Text	1. Algorithm processed for the encryption of data 2. The cipher text retrieved 3. Cipher text together with subsequent plain text and key chosen by the cryptanalysts. 4. Plain text together with subsequent cipher text and key chosen by the cryptanalysts.
Cipher text Only	1. Encryption Algorithm to alter the data 2. Cipher text Retrieved

of a combination of threats and vulnerabilities that affects the messages transferred via the network [8]. Three key principles of network security are Confidentiality Integrity Availability (CIA). When, there is a need to secure the information from unauthorized access then the confidentiality is required there. If an individual succeeds in breaking the site and steal the encrypted information then the integrity of the information is compromised. If any larger organizations would be severely damaged and there is no network commissioned for longer duration, then availability becomes a key concern [9], [18]. The explained Protection of data while transferred via the communication medium is the prime focus by researchers all over the world [3]. The data protection techniques available in the literature are such as creating a data usage policy, access control mechanisms, encryption techniques, by hardening the endpoints and network infrastructure, by physically securing the working environment, periodical backing up of data, by enforcing compliance and by validating the processes etc [10], [28]. Attacks are classified into two major divisions termed as Active attacks and Passive attacks. An active attack involves a deliberate action on the data to gain access to the data thereafter and highly harmful. On the other hand, the passive attack, are employed only to gather any information related to the messages shared and these are easier to detect. The following table 1 shows the list of active and passive attacks. The main suggested, the cloud service provider must guarantee the service level agreements and security to the data in the cloud. The security standards are enforced to avoid disclosure of the data transferred by the cloud. Rather than the private cloud model, all other three application models depend on the third party as the service provider that leads to the development of security mechanisms [27]. Data protection or data privacy is the vital need of every computing paradigm. Specifically, in the area of cloud computing, the third party operates and manages the data; thereby the security of the user data may be breached in the cloud computing archetype. One of the processes of protecting the data through the cloud is by encrypting the data and made it inarticulate [30], [37].

The security and privacy of data attains its more critical importance when a large number of organizations and enterprises use the open communication medium to transfer their messages. The confidentiality and integrity of the data must be guaranteed by the internet service providers at this scenario. Many security mechanisms and techniques have been found by the researchers to ensure the security of data. Among them, cryptography is the Science of keeping the data secure, by enciphering the data to an inarticulate format [10].

The Cryptographic algorithms are characterized by three dimensions, named as encryption, key generation, and the decryption. The Cryptographic algorithms should ensure the confidentiality, authentication, integrity, non-repudiation, and non-replay to the data being transferred through the communication medium represented in Althar and Samanta [3]. The following table 2 categorizes the type of security mechanism to achieve varied services.

The Symmetric key algorithm uses *Feistel* structure for the encryption and decryption process. The knowledge of design principles of the block cipher and a stream cipher is necessary to decide which is to be implemented for the encryption based on the need. Most of the symmetric key encryption allows block cipher encryption where some other allows stream ciphers. The differences between two cipher models were discussed below in the following sections explained. Figure 2 and table 3 shows the list of symmetric key algorithms that are widely used. The block size of 64-bit, 128-bit, and 256-bit is in use. Block ciphers break up the plain text into chunks, combine the key with the chunks and produces cipher text for the same length of chunks. Some algorithms that work on the principle of block ciphers are Blowfish etc. The block chain

is the capability to actions a single message restrict at a time and produces cipher data simultaneously [6], [38].

The block cipher modes were created to keep from having the same plain content block always encrypting the same cipher content block. Such blocks are called as reversible, or non-singular. The block diagram is shown in figure 2. If the order of sequence changes then the whole stream will be collapsed. Padding is not required in the stream ciphers; they can be of any length. There are numerous stream ciphers and most of them worked on the principle of generating random keys as the seed for the generators presented. Then the stream of plain text is *exclusively-ORed* with the plain text stream and cipher text is created and its structure is presented. [20]. The conventional encryption operations work on block ciphers and encrypt the user define plain text to unreadable form. A block ciphers, obtains fixed-length block size, key size and in turn produces fixed-length cipher blocks [21]. When the plain text data length exceeds the fixed block size, then it is spliced and encryption operation is done. Block ciphers can be applied by five different modes of operations as defined by the *NIST (SP 800-38A)*. This consortium recommends five confidentiality encryption operation modes for symmetric block cipher encryption.This work provides a brief introduction to the network security issues and challenges along with threats and vulnerabilities present in the transmission medium. A proposed the cryptographic algorithms applied to defend the attacks are discussed in detail in this work.The Cipher Block Chaining operation mode is the base for all the three new developed algorithms and focused much. Finally, varied tools used for the cryptanalysis are precisely stated in this work.

III. SYSTEM DESIGN

Business enterprises, Public sectors and the government organizations looking forward for better information technology architecture, to provide agile services to the clients with extended scalability. Cloud computing, a democratization computing potentially establish in its own way in this digital decade and has grown energetically in the field of information technology. Cloud computing gains its name as a metaphor for the network services. The democratization computing facility enables the potential to scale for any application. The cryptographic approach consists of the 4 necessary components namely the plain image/text, cryptosystem, cipher image/text and the key. They are described in table. Generally, Cloud Computing refers to the applications as well as the services run on the distributed network by using virtualized resources that are accessed via the virtualized middle ware architecture, networking standards and internet protocols [11]. More specifically, Cloud computing is an evolving archetype in which computing is migrating from personal computers to large centrally managed data centers. The *NIST* defines, Cloud computing as the internet based computing where the shared servers virtually provide service, software, infrastructure, platform, and other devices and resources to the customers as a metered service.

The Cryptographic algorithms are characterized by three dimensions, named as encryption, value generation, and decryption. Cryptographic approaches should ensure the confidentiality, authentication, integrity, non-repudiation, and non-replay to the data being transferred through the communication medium. The following table categorizes the type of security mechanism to achieve varied services [36]. Cloud computing archetype offers the resources to its users as services. It includes various services such as platform, software, database, protection and infrastructure. The foremost challenge ahead of the cloud computing paradigm is the cloud data security. It is broadly classified as user authentication, data protection and data breach. The data in the storage, either in the server or at user level should be secured from unauthorized access. Cloud computing has all the threats and vulnerabilities associated with the network and also other threats from the pooled, shared and virtualized services. Various circumstances, where there is a need for data security in cloud services are such as Datain- transit, Data-at-rest, accounting procedures, locking down networks, application software used, middle ware incorporated, Data Lineage, Data remanence, and host security. Network security related risks are also related to the cloud [26].

This work explain Support Vector Machine Algorithm is that protocol is population and vector based and makes use of the producer-scrounger model and the Data security. The Producer-scrounger is that design of optimal search scheme which owes its inspiration to animal security behavior and also group living theories [42]. To ensure that it is not forced into the local minimum, the Support Vector Machine Algorithm uses ranger foraging method. The Support Vector Machine Algorithm protocol is referred to as a group and all individuals are members.

The Support Vector Machine Algorithm is referred to as a group and all individuals are members.

- Pheromone value-It is given by the measure of ant that chose demo in recent times.
- Heuristic-It is a issues based measure the encryption.

The choose the trail with the maximum pheromone density and heuristic behaviour. A time variant social and cognitive element will enhance the capacity of this protocol for an encryption. Information pass through any computing medium needs utmost security to protect it from unauthorized threats and attacks. In the present era, almost all the fields including medical transcriptions, educational institutions, Government institutions, private enterprises utilize the Cloud block chaining services [40].

A. TEXT DATA CRYPTOSYSTEM

So for improving the performance of the performance of the SVM the previous stopping strategies are suggested. The rate of error validation has been watched the encryption period. If the error of validation takes place for a particular set iterations process the training to final. As explained in the

TABLE 5. Essential components of the cryptographic system.

Components	Description
Plain text	Original intelligible message fed as input to the cryptographic process
Encryption Algorithm	Various permutations and substitutions on the given plain text
Key	A Secrete values used by the mathematical in encryption and decryption
Cipher text	Scrambled or inarticulate text produced as the output of the cryptographic process
Decryption process	The revoke of the encryption approach is decryption. It consists of mathematical algorithms key to producing the new plain image/text back.
Cryptography	The science mathematics of placing the information as protected
Cryptanalys	The science algorithm of separate the cipher image/text
Cryptanalyst	The practitioners to Cryptanalysis
Cryptology	The class of mathematics combining both the cryptanalysis

TABLE 6. Service offered by the block chain security mechanisms.

Security Mechanism	Services Offered
Cryptography	Confidentiality
Digital Signature Verification and Digital Certificates	Authentication
Identity Management	Integrity
Message Digest and Digital Signature	Non-Repudiation
Hash Technique, Encryption and Digital Signatures	Non-replay

TABLE 7. Mathematical symbols and their descriptions for proposed bio-Inspired encryption algorithm.

| Symbol	Description
$\oplus$	XOR (Exclusive Disjunction Operator)
Z_{xy}	Matrix with x,y Elements (x-row, y-column)
$Y_{in} = Y_0^1, Y_2^2, Y_2^3, \ldots, Y_7^8$	X = I^{st} Matrix , i=Bits form 0-7, n=Elements 1-8
$Y_{in} = Y_0^1, Y_1^2, Y_2^3, \ldots, Y_7^8$	Y= IInd Matrix , i=Bits form 0-7, n=Elements 1-8
R= $R_{n0}^R, R_{n1}^R, R_{n2}^R \ldots R_{n255}^R$	Red Channel (R) with pixel elements 0-255
G =$G_{n0}^G, G_{n1}^G, G_{n2}^G \ldots G_{n255}^G$	Green Channel(G) with pixel elements 0-255
B = $B_{n0}^B, B_{n1}^B, B_{n2}^B \ldots B_{n225}^B$	Blue Channel (B) with pixel elements 0-255
IV = $X_0, X_1, X_2 \ldots X_7$	Initialization Vector
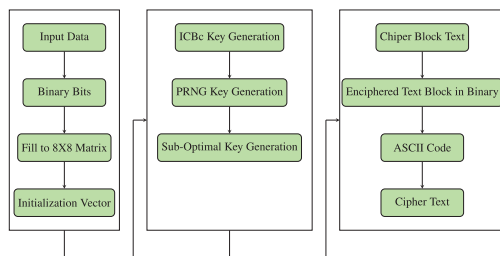
FIGURE 5. Block diagram of text encryption.

section the primary conversion of data is done and their values are placed respectively in the matrix.

It is the responsibility of Cloud service provider, to maintain the standards, policies and security level agreements to its users in a robust way. Security Challenges in the Cloud paradigm include various attacks Initialization Vector, Chosen-Plain text, Cipher Attack, indistinguishably Attacks, Brute-Force attacks, differential and statistical attacks in data encryption [40]. Cloud offers a lot of services regarding the security such as protection service, Encryption service etc.

Network security standards and policies are used for the protection of data and other information stored in the computers. In the distributed computing scenario, three concepts embody the fundamental security objectives namely the confidentiality, Integrity, and availability. Confidentiality involves two important aspects Data privacy and authenticity. The foremost challenge regarding the network security is the attacks that compromise the authenticity of the data owned by the users. Figure 6 explain general proposed system architecture diagram cipher block chain methods. The first and foremost requirement is to verify the type of data which is to be transferred, the type of encryption mechanism applied for the encipherment of the data and the chance of attacks. These limitations are motivated to develop and deploy a cryptographic mechanism as security service, that is to be offered as an application model by the cloud service providers which resists these vulnerabilities [7].

In the block cipher algorithms, the plain text data should be indicated as sequence of bit strings and the cipher text produced will also results Bit-Stream Generation Algorithm Key Cipher text Plain text Encryption Bit-Stream Generation Algorithm Key Plain text as sequence of bit strings. Among all these classifiers, *SVM* classifier is predicting an optimal hyperplane, which is linearly, separates all the features vectors, by projecting on higher dimensional space. *SVM* classifier that calculate the outcome of the unknown sample, by calculating the distance between the unknown point and its nearest neighbor point. Compared with conventional classification methods, *SVM* is used to minimize the empirical training error, minimize. Finally *SVM* classifier provides better results compared with other two methods. The psude code implementation for *SVM* explained in figure 7. The type of data being stored in the cloud takes varied forms such as the text, images, executable files, PDF, library files etc. The cloud service should be capable of resist the attacks on these data when transferred through cloud. In the arena of cloud computing, the third party designs and operates the infrastructure, which rises to the chance of disclosure to the data. The cloud service provider should guarantee the authenticity of the data to be stored or be transferred.

The protection of data is the primary focus of this research work. A new cryptographic algorithm is coined in key sizes. The key generation decides the effectiveness of the algorithm,

---

Algorithm 1: SVM Based Cipher Strategy

Result: Cipher image

1) Set environment, as N->number of seeds = 1945 and get Parents value ;

2) Set random seed streams for N limitation and initialize Mutation Rate= 03;

for $i = 1$ *to length (Parents)* **do**

    1) Child = PopulationParents (i) ;

    2) Mutation_Points = Find (random value (1 to length (child) < Mutation Rate);

    3) range = Population_lnitial_Ramge;

    4) Lower level = range (1, 1 to column);

    5) Upper level = range (2, 1 to column);

    6) Span_level = Upper level − Lower level;

    7) ChildMutation Points = Lower level + random value (1 to length (Mutation_Points)) * Span_level;

  if *size (Child) = size (Unique_Value (Child))* **then**

    | break loop;

  else

    | Goto step 5 ;

  end

end
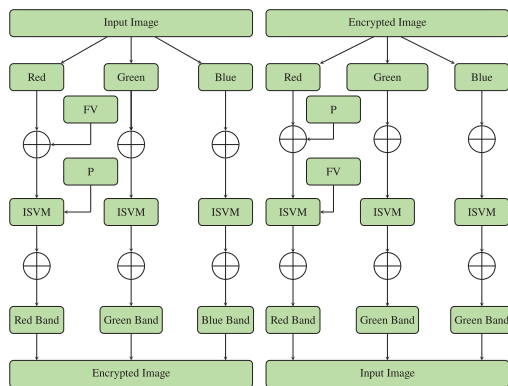
FIGURE 6. Architecture of RGB color image encryption and decryption.

among the three algorithms constructed, in the first algorithm key generation is based on the conventional encryption operation mode and the other two algorithms key generation for encryption is based on optimization technique. Finally, a cloud application model that combines the three cryptographic algorithms and offers it as a security service to the users on cloud is deployed. The application service designed in this research work performs better for protecting the data when stored or transmitted in cloud computing environment.

The also main contribution is the proposed system of Optimized mechanism using the swarm Optimization algorithm. The structure and construction of this enhanced application model using the genetic algorithm for optimized key generation process are explained and its experimental results are verified for varied types of data.security proof for the three cryptographic algorithms constructed and the performance analysis of these algorithms based on several metrics are elaborated. It is presented with security and performance analyses for varied data types. Comparative analysis is done between

the three proposed cryptographic algorithms and also with existing algorithms.

IV. RESULT AND DISCUSSION
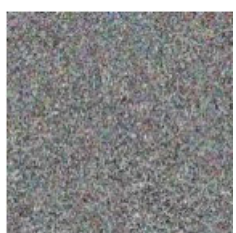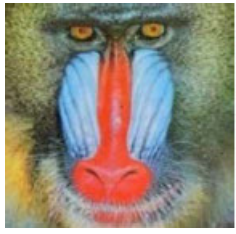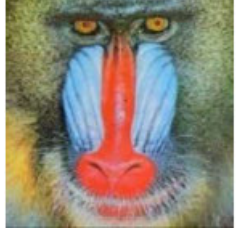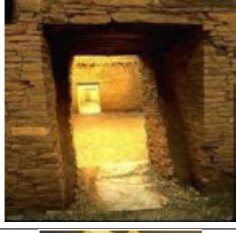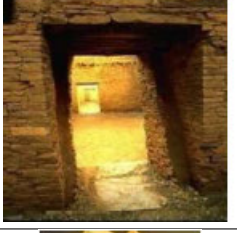
The proposed methodology is applied by making use of *matlab2013a* on Intel(R) Core(TM) i5-2410M CPU 2.30GHz and 16 GB RAM. The performance evaluation of the researcher's proposed Support Vector Machine based optimized tree strategy is done on particular security since it affects lifetime motion inability. The statement of facts relating to jaundice data is collected from different unsorted sources in various ways. Table 8 explain the image encryption for varies image data with varied key formats and table 10 explain the image encryption for varies text data with varied key sizes.

Keys are the vital component, decide the quality of encryption. In this research work, we concentrate on developing a cryptographic algorithm, with strong key generation. In this newly constructed algorithm, three various pairs of key are generated, based on conventional encryption and optimization techniques. This research work *paysan* attention in developing and deploying an application model that offers security. This application model is developed with the objective to afford security services for data by means of *SVM* cryptographic algorithms that resist the several attacks in block chaining. Proposed system also provides the security to varied data that includes text files, Images, and Multimedia Files.

A. TEXT ENCRYPTION

Security and encryption both terms are interchangeably take part throughout the proposed research. The *SVM* encryption, application model imposes a new cryptographic based service that converts the user defined content to unintelligible format. Quality and strength of the newly designed cryptographic algorithm in this research work is analyzed by the key used for

TABLE 8. Encryption and decryption of varied type image data.

Key size	Input images	Encrypted image	Decrypted image
64 bits			
64 bits			
128 bits			
128 bits			
256 bits			
256 bits			

the process. This application model extensively concentrates on the construction of key generation that is computationally secure. Computationally, as the term defines, the key used for the cryptographic process should encompass two important criteria the cost of breaking the cipher data exceed the value of the information encrypted and the time required to break the cipher should surpass the entire life span of the information. Table 10 display the varies file encryption and decryption results according to the key size and file types.

TABLE 9. Encryption and decryption of varied type text data.

Key size	File Size	Input Text Data	Encrypted Data	Decrypted Data
64 bits	126000 (in bytes)	The growth of internet era leads to a major transformation in a storage of data and accessing the applications.	4CLNQtDs16RGY1u9 N5oyhkbV2AlV+CiV MsYqi9AZH9ngcUKu nXzY2ZBErRYD7Cm 5YhKbveTTsSeGBZ7 MxUb/vWtx3rhGJQ==	The growth of internet era leads to a major transformation in a storage of data and accessing the applications.
128 bits	45900 (in bytes)	Cloud Computing is capable of Multitenancy feature that allows the configurable computing resources to be shared by heterogeneous user on -demand. Computing resources offered by the Cloud includes the servers, networks, storage, and applications, all as services.	j+ 6qiUu7wCgaUNB9MHVm3yNiB6qpj6ggAt8t57 jABg0Bf0PbDDB0CL0mwCi2ANtDaJ1GmnD QKH0Kq3SMhL8mlak+ZYveFNP+ 68uQAX3V0prLk07i81z9Y7CUhHN51blrAIK4 FDqRvOOu8u2ojRu+8DqUyl9 +wQvciXaF0SZZxWN4Gy9SkyFm4W+RoLtz XSKrWxldl/JC87DVPG1ziNqyLL0PMf+e2oEp iBJpsfvCcLU20WnFdKIQMkV9f1yMDoJYh1R CAgGfBrLnl1Lytx7emzlmkB5ZWMYvpwUitjh 7Kg95kUmnSxv2P5ipH1xUgeb/UbqvbxsdIVIg5 fng3j0L51RKzi6lSHLaxS8i8+uBNI=	Cloud Computing is capable of Multitenancy feature that allows the configurable computing resources to be shared by heterogeneous user on - demand. Computing resources offered by the Cloud includes the servers, networks, storage, and applications, all as services.
256 bits	85300 (in bytes)	In case of images, it resists well against statistical and differential attacks. Comparative Analysis shows evidence of the efficiency of the developed pioneering application model quality and strength compared with that of the existing services……	DvXGQXu4D1jBmLG5pYm+W8jIkTFp rawOiZJnLXkCgMBM7SF8YMpTMW3 sZIXGK23ygA3m1yVf1GI1NHfxxl+Q5p lF8wKDo9X3rcWAWF9wKwj/ww/BnCi pQKvxdQx357d/5fVzjYVY3XXLThjlC O/C3nGd27M3z7YbNwxOiIxhaAWL3e PavwjA76irzNYclGitB/lYjiZgbzcOislGPa LZe87dN9TmO+FHAqpmB3Rvx8Cr0H EXI7yFekRacIERRT+qv4SfcAhcrbtC8R QLvISeGJkHzwoHQPNfZTMTGlOzj0Be q3eClq1rl+wiupkFyTIB0TfS4jsEsgdeqO Cj4+QYdA==……	In case of images, it resists well against statistical and differential attacks. Comparative Analysis shows evidence of the efficiency of the developed pioneering application model quality and strength compared with that of the existing services……

TABLE 10. Encryption and Decryption of varied files.

File Size (in Bytes)	File Type	Key Size	Encryption Time (in ms)	Decryption Time (in ms)
30706	Executable	128 bits	4.912	4.933
423195	*DLL*	64 bits	4.8	4.91
774018	Document	128 bits	1.02	1.24
1996745	PDF	64 bits	1.9	2.1
157604818	AVI	256 bits	4.983	5.867

The main objectives of this application model are to provide computationally secure key generation to protect the data via encryption. This key generation in the cryptographic process falls into three categories in this research work. In the part, *SVM* encryption service model is constructed for which the key generation is from the conventional encryption operation mode with some improvements. To make the process more complex, the optimization techniques are taken into account for the key generation in descendant two methods. Altogether the three methods are assembled as the *SVM* security, application model that acts computationally more secure specifically for Cloud environment.

B. COMPARATIVE ANALYSIS
The performance of the application model service including three various encryption schemes is analyzed using several metrics for statistical attacks, differential attacks etc. The following objectives behind this proposed algorithm is to minimize the execution time and to produce sub-optimal keys for cryptographic process. Designing this *SVM* algorithm is to minimize the execution time and storage space capacity. In proposed cloud computing techniques, the space complexity is prominent issue; it is almost minimized with by converting the contents to binary bits in this method. Cloud computing has all the threats and vulnerabilities associated with the network and also other threats from the pooled, shared and visualized services. Various circumstances, where there is a need for data security in cloud services are such

TABLE 11. Comparative analysis of text encryption for varied Key size.

2*Key Sizes	2*File Size (Bytes)	Encryption Time(ms)	
		GA Algorithm	SVM algorithm
64 bits	85300	0.079	0.058
128 bits	85300	0.048	0.031
256 bits	85300	0.013	0.011

as Data in-transit, Data-at-rest, accounting procedures, locking down networks, application software used, middle ware incorporated, Data Lineage, Data permanence, and host security. Table 11 shows the variations in time seconds between the existing GA and proposed *SVM* algorithms for varied key sizes. Three most important component of the cryptography mechanism is encryption, key generation, and decryption. The cryptographic algorithm designed should be capable of performing security related renovation, in such a way that the adversary should not overwhelm. The proposed block chain cloud service should be capable of resist the attacks on these data when transferred through cloud. In the arena of cloud computing, the third party design sand operates the infrastructure, which rises to the chance of disclosure to the data also text encryption time need to elaborate system functions.

Figure 7 explain the proposed system in terms of 64 bits, 128 bits, and 256 bits of key sized to resulting time of encryption are displayed. Our proposed system clearly indicate the better result in the form of all three types of key values. The proposed cloud service provider should guarantee the authenticity of the data to be stored or be transferred.
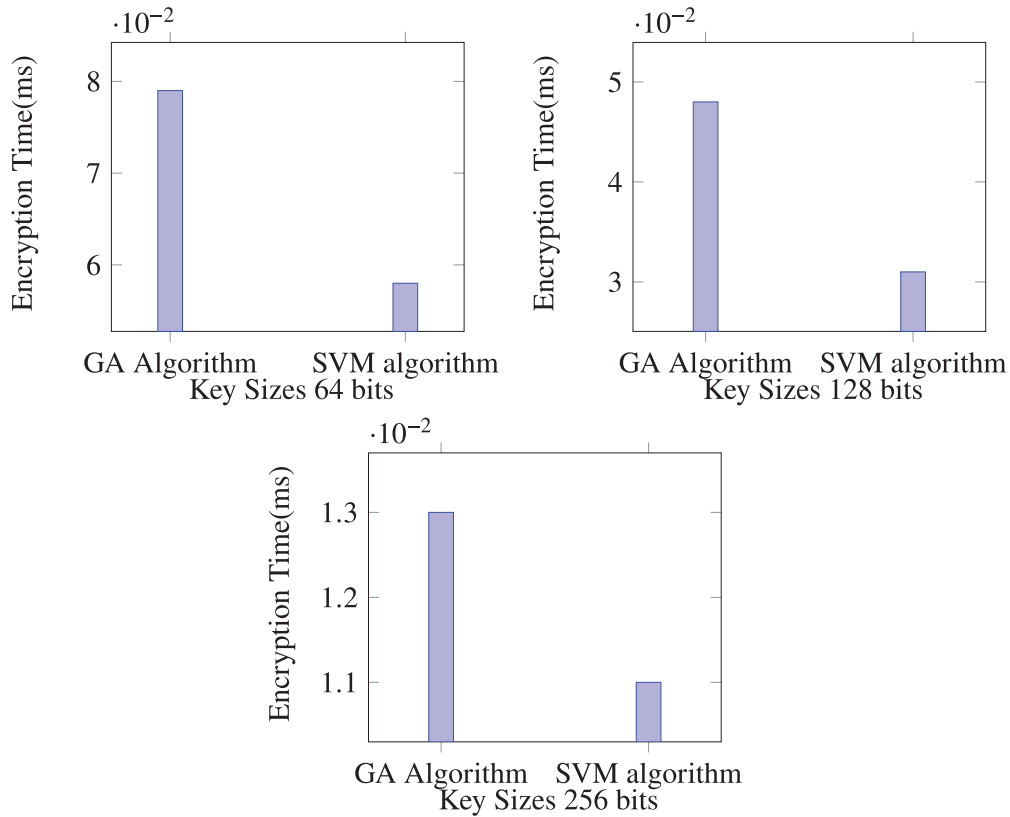
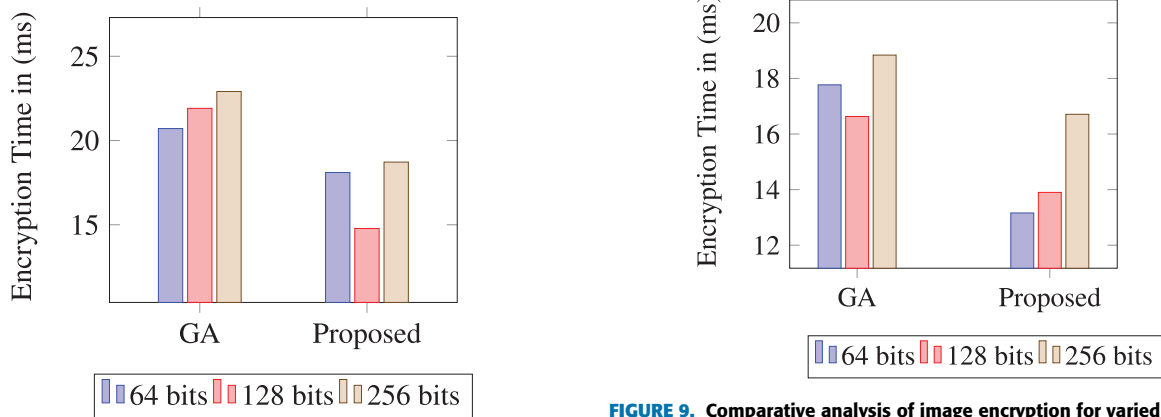**FIGURE 7.** Comparative analysis of text encryption for varied Key.

FIGURE 8. Comparative analysis of image encryption for varied key size for BMP images.

FIGURE 9. Comparative analysis of image encryption for varied key size for JPEG images.

Main aim of designing proposed algorithms is to minimize the execution time and maximizes the scalability. The application service designed in this research work performs better for protecting the data when stored or transmitted in cloud computing environment. Notable feature of this contribution is that, key optimization is done by the nature inspired *SVM* algorithm. The experimental results demonstrate that the proposed application model outperforms traditional cloud encryption services by analyzing several metrics such as

entropy and chi-square test. This work, application model deployed in this research work is comprised of the new cryptographic algorithms and its implementation, access control grants details are listed and experimental results are described in concise.

V. CONCLUSION

The results of security analysis confirm the effectiveness of the proposed application model withstands potentially against various attacks such as *Chosen Cipher Attack*, Chosen plain text attack indistinguishably attacks for files. In case

of images, it resists well against statistical and differential attacks. Comparative Analysis shows evidence of the efficiency of the developed pioneering application model quality and strength compared with that of the existing services. Security mechanism like the cryptography that protects data from unauthenticated access is explained in brief. Cloud computing fundamentals and its application models are discussed in crisp. Data security in cloud computing is focused primarily, and the motivation behind this research work is presented. From the result part provide the comparison between the existing and proposed system design explained the execution time and scalability of result are provided, proposed encryption methods are suitable for both image and text encryption standard. The security proof for the three cryptographic algorithms constructed and the performance analysis of these algorithms based on several metrics are elaborated. It is presented with security and performance analyses for varied data types.

REFERENCES

[1] C.-M. Chen *et al.*, "A secure blockchain-based group key agreement protocol for IoT," *J. Supercomput.*, pp. 72–78, Feb. 2021, doi: 10.1007/s11227-020-03561-y.

[2] R. R. Althar and D. Samanta, "The realist approach for evaluation of computational intelligence in software engineering," *Innov. Syst. Softw. Eng.*, vol. 17, no. 1, pp. 17–27, Mar. 2021.

[3] B. Rodrigues *et al.*, "A blockchain-based architecture for collaborative DDoS mitigation with smart contracts," in *Proc. 11th IFIP Int. Conf. Auton. Infrastruct., Manage. Secur. (AIMS)*, Zürich, Switzerland, Jul. 2017, pp. 16–29. [Online]. Available: https://ff10.1007/978-3-319-60774-0_2ff

[4] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2018.

[5] A. K. Biswal, D. Singh, B. K. Pattanayak, D. Samanta, and M.-H. Yang, "IoT-based smart alert system for drowsy driver detection," *Wireless Commun. Mobile Comput.*, vol. 2021, Mar. 2021, Art. no. 6627217.

[6] J. Biswas, P. Kayal, and D. Samanta, "Reducing approximation error with rapid convergence rate for non-negative matrix factorization (NMF)," *Math. Statist.*, vol. 9, no. 3, pp. 285–289, May 2021.

[7] F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform.*, vol. 36, pp. 55–81, Mar. 2018.

[8] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, nos. 6–10, p. 71, 2016.

[9] V. Dhanush, A. R. Mahendra, M. V. Kumudavalli, and D. Samanta, "Application of deep learning technique for automatic data exchange with air-gapped systems and its security concerns," in *Proc. Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Jul. 2017, pp. 324–328.

[10] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[11] X. Fu, H. Wang, and Z. Wang, "Research on block-chain-based intelligent transaction and collaborative scheduling strategies for large grid," *IEEE Access*, vol. 8, pp. 151866–151877, 2020.

[12] G. Kumar, R. Saha, M. Rai, R. Thomas, and T. H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.

[13] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology—EUROCRYPT*. Cham, Switzerland: Springer, 2015, pp. 281–310.

[14] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, "Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 4995–5001, Nov. 2020.

[15] A. Guha and D. Samanta, "Hybrid approach to document anomaly detection: An application to facilitate RPA in title insurance," *Int. J. Autom. Comput.*, vol. 18, no. 1, pp. 55–72, Feb. 2021.

[16] A. Guha, D. Samanta, A. Banerjee, and D. Agarwal, "A deep learning model for information loss prevention from multi-page digital documents," *IEEE Access*, vol. 9, pp. 80451–80465, 2021.

[17] D. S. Gupta, S. H. Islam, M. S. Obaidat, A. Karati, and B. Sadoun, "LAAC: Lightweight lattice-based authentication and access control protocol for E-health systems in IoT environments," *IEEE Syst. J.*, early access, Sep. 21, 2020, doi: 10.1109/JSYST.2020.3016065.

[18] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: Security issue in IoT network," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC), 2nd Int. Conf.*, Aug. 2018, pp. 104–107.

[19] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[20] R. T. Hasanat, M. Arifur Rahman, N. Mansoor, N. Mohammed, M. S. Rahman, and M. Rasheduzzaman, "An IoT based real-time data-centric monitoring system for vaccine cold chain," in *Proc. IEEE East-West Design Test Symp. (EWDTS)*, Sep. 2020, pp. 1–5.

[21] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, Z. Wen, and X. Qi, "Block chain based Internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT u6 HCS)," *IEEE Access*, vol. 8, pp. 216856–216872, 2020.

[22] J. Lee, M. Azamfar, and J. Singh, "A blockchain enabled cyber-physical system architecture for industry 4.0 manufacturing systems," *Manuf. Lett.*, vol. 20, pp. 34–39, Apr. 2019.

[23] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[24] V. K. Verma, "Blockchain technology: Systematic review of security and privacy problems and its scope with cloud computing," *J. Netw. Secur.*, vol. 7, no. 1, pp. 1–6, 2019.

[25] A. Khamparia, P. K. Singh, P. Rani, D. Samanta, A. Khanna, and B. Bhushan, "An Internet of health things-driven deep learning framework for detection and classification of skin cancer using transfer learning," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 7, 2020, Art. no. e03963.

[26] S. Khan, M. A. Irfan, A. Arif, A. Ali, Z. A. Memon, and A. Khaliq, "Reversible-enhanced stego block chaining image steganography: A highly efficient data hiding technique," *Can. J. Electr. Comput. Eng.*, vol. 43, no. 2, pp. 66–72, 2020.

[27] J. M. Kizza, *Guide to Computer Network Security*. Berlin, Germany: Springer, 2015.

[28] R. Kumar, R. Kumar, D. Samanta, M. Paul, and V. Kumar, "A combining approach using DFT and FIR filter to enhance impulse response," in *Proc. Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Jul. 2017, pp. 134–137.

[29] L. Zhu, Y. Wu, K. Gai, and K.-K.-R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Gener. Comput. Syst.*, vol. 91, pp. 527–535, Feb. 2019.

[30] J. Mahalakshmi, K. Kuppusamy, C. Kaleeswari, and P. Maheswari, "Iot sensor-based smart agricultural system," *Springer Sci. Bus. Media LLC*, 2020.

[31] M. Maheswari, S. Geetha, S. S. Kumar, M. Karuppiah, D. Samanta, and Y. Park, "PEVRM: Probabilistic evolution based version recommendation model for mobile applications," *IEEE Access*, vol. 9, pp. 20819–20827, 2021.

[32] M. S. Mekala, R. Patan, S. H. Islam, D. Samanta, G. A. Mallah, and S. A. Chaudhry, "DAWM: Cost-aware asset claim analysis approach on big data analytic computation model for cloud data centre," *Secur. Commun. Netw.*, vol. 2021, May 2021, Art. no. 6688162.

[33] B. Praveen, N. Umarani, T. Anand, and D. Samanta, "Cardinal digital image data fortification expending steganography," *Int. J. Recent Technol. Eng.*, vol. 8, no. 3, pp. 163–172, 2019.

[34] P. Punithavathi, S. Geetha, M. Karuppiah, S. K. H. Islam, M. M. Hassan, and K.-K. R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," *Inf. Sci.*, vol. 484, pp. 255–268, May 2019.

[35] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[36] M. Rathor and A. Sengupta, "IP core steganography using switch based key-driven hash-chaining and encoding for securing DSP kernels used in CE systems," *IEEE Trans. Consum. Electron.*, vol. 66, no. 3, pp. 251–260, Aug. 2020.

[37] D. Samanta, M. G. Galety, M. Shivamurthaiah, and S. Kariyappala, "A hybridization approach based semantic approach to the software engineering," *TEST Eng. Manage.*, vol. 83, pp. 5441–5447, Mar. 2020.

[38] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 6, pp. 996–1010, Nov./Dec. 2019.

[39] P. Sivakumar, R. Nagaraju, D. Samanta, M. Sivaram, M. N. Hindia, and I. S. Amiri, "A novel free space communication system using nonlinear InGaAsP microsystem resonators for enabling power-control toward smart cities," *Wireless Netw.*, vol. 26, no. 4, pp. 2317–2328, May 2020.

[40] H. Treiblmaier and C. Sillaber, "A case study of blockchain-induced digital transformation in the public sector," in *Blockchain and Distributed Ledger Technology Use Cases*. Cham, Switzerland: Springer, 2020, pp. 227–244.

[41] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020.

[42] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, "An overview of blockchain security analysis," in *Proc. China Cyber Secur. Annu. Conf.*, 2019, pp. 55–72.

[43] X. Liang, S. S. Shetty, D. Tosh, L. Njilla, C. A. Kamhoua, and K. Kwiat, "ProvChain: Blockchain-based cloud data provenance," in *Blockchain for Distributed Systems Security*. Hoboken, NJ, USA: Wiley, 2019.

[44] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.

[45] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 9, pp. 1975–1989, Sep. 2019.

Amazon and Flipkart. He has presented various articles at international conferences and received best paper awards. He has authored or coauthored of 19 book chapters. He also serves as an Acquisition Editor for Springer, Wiley, CRC, Scrivener Publishing LLC, Beverly, USA, and Elsevier. He is an Associate Life Member of the Computer Society of India (CSI) and a Life Member of the Indian Society for Technical Education (ISTE). He is a convener, a keynote speaker, a session chair, a co-chair, a publicity chair, a publication chair, an advisory board, and a technical program committee member in many prestigious international and national conferences. He was an invited speaker with several institutions.

AHMED H. ALAHMADI received the Ph.D. degree in computer science and engineering from La Trobe University. His Ph.D. research was in e-health business requirements engineering. Since then, he has published various peer-reviewed research articles. He worked as the Dean of the College of Computer Science and IT, Al-Baha University. He is currently an Assistant Professor with the Department of Computer Science and Information, Taibah University, Saudi Arabia, where he is also the Dean of the Khaybar Community College. In addition to research, he is also skilled in accreditation and college recruiting. His research interests include e-health, software engineering, business process modeling, requirements engineering, and process mining. He also has a demonstrated history of working in the higher education industry.

KARTHIKEYAN M. P. is currently an Assistant Professor of computer science with the PPG College of Arts and Science, Coimbatore, Tamilnadu. His research interest includes artificial intelligence medical imaging query processing.

DEBABRATA SAMANTA (Member, IEEE) received the bachelor's degree (Hons.) in physics from Calcutta University, Kolkata, India, the M.C.A. degree from the Academy of Technology, West Bengal University of Technology (WBUT), West Bengal, and the Ph.D. degree in computer science and engineering from the National Institute of Technology, Durgapur, India, in the area of SAR image processing. He is currently working as an Assistant Professor with the Department of Computer Science, CHRIST (Deemed to be University), Bengaluru, India. He is keenly interested in interdisciplinary research and development and has experience spanning fields of SAR image analysis, video surveillance, heuristic algorithm for image classification, deep learning framework for detection and classification, blockchain, statistical modeling, wireless *ad-hoc* networks, natural language processing, V2I communication. He has successfully completed six consultancy projects. He has received funding under International Travel Support Scheme, in 2019, for attending conference, in Thailand. He has received Travel Grant for speaker in Conference and Seminar for two years, in July 2019. He is the owner of 18 patents (two design Indian patent and two Australian patent granted, 14 Indian patent published) and two copyright. He has authored or coauthored over 151 research articles in international journals (SCI/SCIE/ESCI/Scopus) and conferences, including IEEE, Springer, and Elsevier Conference proceeding. He has received "Scholastic Award" at 2nd International Conference on Computer Science and IT application, CSIT-2011, Delhi, India. He is a coauthor of ten books and the co-editor of five books, available for sale on

MOHAMMAD ZUBAIR KHAN received the M.Tech. degree in computer science and engineering from Uttar Pradesh Technical University, Lucknow, India, in 2006, and the Ph.D. degree in computer science and information technology from the Faculty of Engineering, Mahatma Jyotiba Phule Rohilkhand University, Bareilly, India. He was the Head and an Associate Professor with the Department of Computer Science and Engineering, Invertis University, Bareilly. He has more than 15 years teaching and research experience. He is currently an Associate Professor with the Department of Computer Science, College of Computer Science and Engineering, Taibah University. He has published more than 40 journals articles and conference papers. His current research interests include data mining, big data, parallel and distributed computing, theory of computations, and computer networks. He has been a member of the Computer Society of India, since 2004.

AMIT BANERJEE received the Ph.D. degree in semiconductor technology from the Energy Research Unit, Indian Association for the Cultivation of Science (D.S.T., Government of India). He joined the Advanced Device Research Division, Research Institute of Electronics, Japan, as a Scientific Researcher, in 2016. He was also part of the Innovative Photonics Evolution Research Center, Hamamatsu, Japan. He later joined the Microelectronic Technologies and Devices, Department of Electrical and Computer Engineering of the prestigious National University of Singapore, as a Scientist, in 2017. He is currently working with the Physics Department, Bidhan Chandra College, Asansol, West Bengal, India. He is also a member of more than 40 international advisory boards with global MNCs, deep-tech startups, technical program committees, in various countries, coauthored several scientific articles, presented in several international conferences, as a plenary and a keynote speaker. He received seven international awards, authored and edited nine deep-tech books with prominent international publishers. He has extensively worked on design and development of high vacuum plasma CVD reactors, which are used in industrial manufacturing of solar cells, coatings, and TFTs. His recent work on antenna-coupled microbolometer arrays, are compatible with the state-of-the-art medium-scale semiconductor device fabrication processes, and technologically competitive with commercial viability as on-chip integrable detector arrays for terahertz imaging.

GOUTAM KUMAR DALAPATI received the Ph.D. degree from Jadavpur University, Calcutta, India, in 2005. From 2007 to 2018, he was attached with the Institute of Materials Research and Engineering (IMRE), Agency for Science, Technology and Research, Singapore. He has contributed 150 SCI indeed articles and two book as an editor. He has developed highly transparent low cost energy saving coating for smart windows. He has developed the copper oxide as highly photoactive materials for photovoltaic and solar light driven hydrogen production through water splitting. He is currnetly working on advanced materials for sustainable renewable energy generation, energy storage devices, low power devices, smart coating, and blockchain-based technology for circular economy.

SEERAM RAMAKRISHNA (Senior Member, IEEE) is currently a Senior Professor and a Chair of Circular Economy Taskforce withthe National University of Singapore (NUS), which is ranked among the top 11 universities in the world. He is named among the World's Most Influential Minds and the Top 1% Highly Cited Researchers by Thomson Reuters and Clarivate Analytics. He has coauthored 1900 SCI journal articles and ten authored books, which received 123 929 citations and 162 H-index. He is a member of Enterprise Singapore NMC on ISO/TC323 on Circular Economy. He is a fellow of U.K. Royal Academy of Engineering (FREng). He is an Elected Fellow of major professional societies and academies of Singapore, India, U.K., and USA. He chairs the Future of Manufacturing Technical Committee with the Institution of Engineers, Singapore. He is an Advisor with Singapore National Environmental Agency's CESS events.

● ● ●