IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-1, Jan 2019 E-ISSN: 2347-2693

Hybrid Elliptic Curve Cryptography for Secured Cloud Computing

G. Sakthivel[1*], P. Madhubala[2]

[1]Department of Computer Science, Periyar University, Salem, India
[1]PG Department of Computer Science, Arignar Anna College (Arts & Science), Krishnagiri, India
[2]PG & Research Department of Computer Science, Don Bosco College, Dharmapuri, India

[*]*Corresponding Author:sakthishc@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 20/Jan/2019, Published:31/Jan/2019

Abstract— This paper presents a secure cloud storage scheme based on hybrid cryptosystem, which consists of Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), and one-way hash function. Here, the data owner exports large volume of encrypted data to a cloud storage provider, the Electronic cryptography is a public key or asymmetric key means that the encryption key and decryption key are different. In many applications like military databases confidential video conferencing, medical imaging system, online personal photograph album security is very essential. Also, in industrial process wide usage of images can turn it into a resource and asset. So, it is important to protect confidential images data from unauthorized access. this paper proposes elliptical curve cryptography-based security mechanism and ant colony optimization based secured key management technique. The proposed system provides better space complexity than existing RSA and CRT, and the ACO improves optimality.

Keywords*: cloud computing, security, RSA algorithm, elliptic curve cryptography, ant colony optimization.*

I. INTRODUCTION

Secured cloud is an important research issue as it deals with variety of customers, and various devices and metrics. Smaller size of security keys will be preferred as the clouds are accessed by many handheld devices. So the important point which comes to mind is the security with small key size [6]. Cryptography has become one of the major sciences in the present era. The importance of cryptography comes from the intensive digital transactions which we daily perform on the internet and other communication channels. Cryptography is used in all the well-known applications such as online financial transactions, secured data transfer like war messages.

In networking and communication security ECC plays a very crucial role. Elliptic curve arithmetic reduces the modular exponentiation operation to multiplication operation within a group. The mathematical theories involved in public key cryptography generally include factors decomposition problem of large numbers and discrete logarithm problem in finite field. Elliptic Curve Cryptography covers all relevant asymmetric cryptographic primitives like digital signatures and key agreement algorithms [30]. The function used for this purpose is the scalar multiplication K.P which is the core operation of ECCs. Where k is an integer and P is a point on an elliptic curve. ECC will act as a very efficient algorithm which is extremely computationally efficient which provides fast execution time, needs lesser memory, low bandwidth, and minute energy consumption. . This research paper is organized as follows, Section I contains the introduction of Hybrid Elliptic Curve Cryptography and its importance, Section II Hybrid Elliptic Curve Literature survey, Section III Methodology and Section IV Result and Discussion Section V concludes the paper with future directions.

II LITERATURE SURVEY

The new FPGA architecture for the Elliptic curve for cryptographic co-processor is presented by Wang, et al, (2007), [1]. This co-processor consists of elements operation over a binary finite field, point adding and also the doubling on the specific elliptic curve and also the scalar multiplication. In this co-processor the FPGA based modular multiplier framework is proposed for trade-off multiplication between bit serial and bit parallel. The experiment results demonstrated that co-processor designed will achieve utmost performance.

Jarvinen, et al, (2008), discussed about parallelization of different elliptic curve cryptographic accelerators which use the elliptic curves over finite fields [2]. The author provides various tools which can evaluate the use of parallelism and thus show where it can be used to maximize efficiency where special focus was given to a family of curves called Koblitz curves as they can offer high point multiplication efficiency. He has introduced a

new method where the point multiplication latency is reduced by applying the parallel field arithmetic processors. Here very effective elliptic curve cryptography processor architecture is used to get better results than the other existent systems.

A new routing protocol which is proposed by Liu, et al, 2008, which will apply the parallel ant colony algorithm and effectively establish the best path for latent system [3]. The author has described different strategies to exchange the confidential information and run parallel ACO techniques by taking into consideration the source and destination nodes. The proposed protocol reduced the end to end delay and also helps in providing high connectivity without any network scarcity. The packet delivery ratio is very good by this method so it can be easily said that this is much better than the earlier approaches.

Han, et al, 2008, presented a novel grid resource mechanism in which an agent based decentralized grid is used [4]. The algorithm ensured that the coordination and cooperation between the neighbouring nodes is effectively used for efficient problem-solving capabilities. The proposed algorithm is studied by investigating the relationship between semantic similarity and success probability by taking into consideration different factors. The proposed algorithm provided better flexibility and can dynamically discover resources.

The Mobile Agent Based Open Cloud Computing Federation mechanism is presented by Zhang, et al,2009, [5]. This method has the advantages of both cloud computing and the mobile agent. MABOCCF will effectively span in different cloud computing platforms. This method can effectively realize interoperability and portability. This novel method will act as the beginning of an open cloud computing.

Athavale, et al, 2009, has proposed a varied scheme which uses the private redefined credentials of existing elliptic curve cryptography [6]. The proposed method will reduce the multiplication operations and modular exponentiation within a group. The elliptic curve which varies over a finite field Fq will effectively use the private credentials which in turn will help in improving the efficiency of elliptic curve cryptography. This novel method provides results which are very effective and better than the existing systems.

Greenberg, et al, 2009, has proposed methods to reduce cost of data center in cloud environments [7]. To address the problems the author proposed to increase the agility with in a network, give various incentives which can be effectively used for resource consumption. The data centers and networks can be optimized together and new mechanisms and systems for geo-distributing state are identified.

Armbrust, et al, (2010), proposed his research study to focus on various virtualized resources which will be very effective than single node performance [8]. The author studied that the software which uses various applications must have the ability to scale down and scale up rapidly and they can be effectively used in the virtual machines for better results. He focused mainly on Business continuity and service availability.

Binary representation is a new effective way which is proposed by Pathak, et al, 2010, [9]. „DRM" which is the direct Recoding Method is the algorithm which computes the signed binary representation. The method proposed by him is efficient when the other existent methods and are compared with and the experimental results proved the same.

Dinh, et al, 2011, proposed an analysis that during the integration of cloud computing into the mobile environment few obstacles need to be resolved like the performance, environment and security [10]. He also stated that the mobile cloud computing can be effectively applied to a wide range of mobile services which has eventually pushed the revenue of existing mobile cloud computing to $5.2 billion thus analysing its importance.

Zhang, et al, 2011, described hybrid technique which will use an optimized method of Montgomery multiplication. This method takes into consideration the low weight of primes which will minimize the execution time [11]. The author also developed an improved variety of the MAC operation which is integrated with the inner loop of the hybrid method and multiplication, squaring function for the OPFs.

Ant colony optimization (ACO) and its implementation to a fuzzy controller (FC) design was proposed by Juang, at el, 2011, [12]. This method is called as ACO-FC. This method has effectively improved the performance and design efficiency and also for ACO hardware implementation. The ACO is used in ACO-FC is an extension of the known ant colony system the hardware is implemented in the programmable array chip. The ACO chip application is effectively used in the FC of simulated water bath temperature control problem. The method has also bettered the chip design effectiveness.

The problem of mobile sensor networks is used efficiently in single target tracking which is presented by Mourad, et al, 2011 [13]. In the proposed methodology estimating the single target and the position in which targets are currently present is identified. Different estimations are then made to identify the positions with which the targets can be predicted. Once the area is identified the proposed approach will move the mobile nodes which have the capability to identify the optimal path.

Jiang, et al, 2011, presented a new ACO method which is metaheuristic [14]. This method is a novel design where it is effectively used in pumping powers. With this novel method ACO is applied to pump wavelengths to get maximum gain better benefit with the parameters of the existing system.

Jarschel, et al, 2011, presented the Cloud gaming experience [15]. The quality of the cloud gaming experience is measured with different available emulators. A measurement of different services and tests are identified with this new gaming model and the user experience for this is taken into utmost consideration. There will be the influence factors which are known as the key influence factors which are studied along with the content and have the capability to influence different target audience.

A different framework for the decentralized grid is proposed by Hassan, et al, 2011,[16]. The framework implemented the peer to peer architecture which an agent model, ontology model and different algorithms use and they be in constant search of shared resources. His research work states that the key features namely decentralization, scalability and efficiency are implemented in a framework.

An elastic application model for using cloud resources was proposed by Zhang, et al, 2011,[17]. The transparent use of cloud resources is important to know the augmentation capability of mobile devices when there is resource constraint. Different elasticity patterns and cost-effective models are applied to obtain efficient results. The author implemented the framework for the smart phone device which was developed by the set of different elastic applications.

Lili, et al, 2012, proposed a secret sharing technique which is based out of Elliptic Curve ElGamal (EC-ElGamal) [18]. The encryption scheme has an additive homomorphism feature which can be used for secure transmissions as well as for unsecured channels where secret sharing of images can be done efficiently. The proposed scheme enables better performance and relatively shorter key size than the existing schemes such as RSA or ElGamal.

Vigili, et al, 2012, proposed a novel algorithm by implementing Elliptic Curve Cryptography in which transforming the existing message into an affine point on the Elliptic Curve, over the finite prime field is considered [19]. The author illustrated the process of encryption/decryption of a text message and image files in spatial domain by enhancing security using Comparative Linear Congruential Generator for better random number generation which enables the breaking of cipher text impossible for any brute force attack.

Tawalbeh, et al, 2012, identified that the unique characteristics of the elliptic curve cryptography (ECC) which are namely small key size, bandwidth friendly, high speed computations [20]. These features make it very attractive for the use in multimedia encryption. In this study, ECC is used to perform encryption and also multimedia compression. The two ECC based encryption algorithms which were introduced here are applied before and during compression and the results stated that post implementation this method can be used in place of existing methods.

Bitcoin is a digital currency which is widely used in attracting a significant number of users. Barber, et al, 2012, [21] discussed some overview which makes people to understand as to why Bitcoin became so successful. E cash which is a key research topic on cryptographic does not lead to a large-scale deployment. The author identified different issues and attacks of Bitcoin, and proposed various techniques to address them.

Bai Qing-hai, et al, 2012,[22] discussed some overview about the elliptic curve public key cryptography and its design principles. The important contents are researched in the system, and various implementation details of the selection method are identified. The author stated that when the public key is short and when there is fewer networks bandwidths then the ability to resist various attacks are strong.

Pehlivanoglu, et al, 2012,[23] developed an optimization algorithm which is named as multi-frequency vibrational genetic algorithm (mVGA). This method help solve the path planning problems. The path planning problems of autonomous unmanned aerial vehicles (UAVs) is improved significantly. The algorithm emphasized on an application strategy for mutation.

Load balancing on cloud is important and the latest method which uses Ant colony optimization to resolve the problem cloud environment which is presented by Mishra, et al, 2012, [24]. The author proposed a new heuristic algorithm based on ant colony optimization which initiates the load distribution to different services is presented which will use the cloud computing architecture. The pheromone update mechanism proved to be of significant importance when load balancing is considered. The make span is also minimized for cloud-based services.

Cloud mobile media (CMM) services are presented by Dey, et al, 2012, [25]. The author looked at the benefits, early trends, opportunities which paved the way for near future. He analysed the important issues to be addressed, impact of the services which make CMM services viable where cost, privacy, efficiency and effectiveness are taken into consideration. He proposed extending the Cloud to

different wireless networks which were clearly beyond the traditional Internet means.

SSL acts as a protocol for effectively managing the security when a message is transmitted over the Internet. Most web browsers as web server products use this SSL feature. An SSL VPN connection between the cloud ISP and data centers without a lot of the Public Key Infrastructure (PKI) overhead forms the basis of VPN solution that comes from an IPsec which is presented by Kokku, et al, 2012,[26].

A multi-objective ant colony system algorithm is presented for the virtual machine placement problem in which the main goal is to efficiently obtain a set of non-dominated solutions (the Pareto set) that simultaneously minimize total resource wastage and power consumption. This method is proposed by Gao, at el, 2013[27]. The author improved the effectiveness of algorithm by increasing the learning of ants. His algorithm is suitable for large size of data centers with thousands of VMs. Experiments show that the algorithm outperforms other state-of-the-art algorithms.

Abbas, et al, 2013[28] identified an experimental metrics base framework in which Data Drop (DD) and throughput are measured and analysed for Mobile Ad-hoc Network (MANETs) and Vehicular Ad-hoc Network (VANETs). The proposed system classifies the changing in MANET nodes and VANET vehicles data drop, and throughput. The author identified that the results that in form of high through put and low packet drop DSR shows better performance compared with existing systems in both VANET and MANET. The performance parameter includes the Data Dropped and throughput

Fernando, et al, 2013,[29] proposed his research study on different issues of mobile computing. He identified that increasing usage of cloud computing over mobile has its potential difficulties and exploiting the full potential becomes difficult due to its inherent problems such as resource scarcity, frequent disconnections, and mobility. The author in this work stated that mobile cloud computing has overlapped with peer to peer computing, application partitioning and other key areas but has its own set of challenges.

Ahmed, et al, 2013, [30] identified an efficient hybrid image encryption scheme which is based on chaotic system and cyclic elliptic curve. The new defined scheme generates an initial key stream which uses the external secret key of 256-bit and chaotic system in a feedback manner. Then, the generated key streams are mixed with key sequences defined from the cyclic elliptic curve points. Thorough encryption techniques and performance evaluations are done.

A new novel method is proposed by Seo, et al, 2013, [31] i.e., "Carry-Once". The author focuses more on intermediate results rather than the complete results. The performance improvements are identified for ordinary multi-precision multiplications which excluded "product-scanning". The proposed method improved the existing multi-precision multiplication techniques which have intermediate result computation and show greater performance improvements in terms of speed by up to 2.5% which is very efficient

Arshad, et al, 2013, [32] did a cryptanalysis of Tsai"s scheme. The Tsai"s scheme is most vulnerable where password guessing and stolen verifiers are considered. Furthermore, Tsai"s scheme does not provide forward secrecy and known-key secrecy. Then a novel and secure mutual authentication scheme is proposed which is based on elliptic curve discrete logarithm problem for SIP which is immune to the presented attacks.

Encryption technique based on elliptic curves for securing images to transmit over public channels is addressed by Soleymani,et al, 2013,[33]. This cryptosystem utilizes a new mapping method which converts pixel to a point in a plain image where ECC based encryption is taken into consideration. This method proved very efficient compared to all the existing methods.

An image encryption algorithm based chaotic Jacobian elliptic maps is presented by Behnia, et al, 2013, [34]. Some security analysis was presented which illustrates the effectiveness of the proposed scheme. The proposed image encryption technique can be applied for real time applications. The Jacobian elliptic maps which are presented aims at both image encryption and video encryption.

Improved protocol for SIP authentication by using elliptic curve cryptography is proposed by Irshad, et al, 2013, [35] that encounters treats where even enhanced security means are present. Where higher security requirements are needed this analysis will prove very effective.

Security notions and an evaluation of an ID-based ring signcryption scheme for wireless sensor networks were developed by Sharma, et al, 2013,[36]. The proposed scheme by the author was found to be securing against adaptive chosen cipher text ring attacks and also secure against the existential forgery for adaptive chosen message attacks. He also included an analysis of existing schemes and calculated results of the proposed scheme for wireless sensor networks.

Wang, et al, 2013, [37] presented a bionic optimization algorithm-based dimension reduction method named Ant Colony Optimization -Selection (ACO-S) is proposed for

high-dimensional datasets. Because microarray datasets comprise tens of thousands of features (genes), they are usually used to test the dimension reduction techniques. ACO-S consists of two stages in which two well-known ACO algorithms, namely ant system and ant colony system, are utilized to seek for genes, respectively. In the first stage, a modified ant system is used to filter the non-significant genes from high-dimensional space, and a number of promising genes are reserved in the next step. In the second stage, an improved ant colony system is applied to gene selection finally concluded that for high-dimensional datasets this can be effectively used.

A novel ant colony optimization for rule classification was proposed by Shahzad, et al, 2013, [38]. Several datasets are taken into consideration and different parameters are considered for obtaining benchmarks i.e subject and comparison. The high accuracy and comprehensibility of rule sets which are discovered by this algorithm are the major advantages.

A new EBS model is identified by Chen et al, 2013,[39]. EBS adjusts the allocation of various employees at different events. The proposed allocation will change during events and unchanged at non-events thus enabling the flexibility and task conflicts. The author stated that as human conflicts are the major cause of concern so this planning problem, an ACO algorithm is further designed to improve the efficiency.

To obtain a minimal traveling route for a given set of attractions Zhanchang, et al, 2013, [40] improved the existing Ant Colony Algorithm. The author took varied parameters and improved the precision made and the inspired factor was also changed to get better results. Experimental analysis is done after selecting different series of attractions in Beijing which were taken as the base data. The optimum route for travelers is obtained and results stated that the improvements are reasonable and effective.

Lie, et al, 2013, [41] proposed a new model for cloud service selection by aggregating the information from the cloud users as well as from the third party which is used. The author first proposed a framework where the cloud service selection approach is defined. Then the classification of objective and subjective assessment is done and cloud selection approach assessment through a fuzzy simple additive weighting system is done.

A novel approach for the mapping DAG applications is given by Ijaz, et al, 2013[42]. The algorithm uses the list scheduling. The author compared the proposed method with the well-known list scheduling algorithms which are existing in the real world. The comparison results state that the real-world graphs can effectively use the proposed algorithm as this method outperforms the existing ones significantly if both the performance with respect to cost are taken into consideration.

A algorithm to identify the behavior trust evaluation system is proposed by Guoyuan Lin, et al, 2014,[43]. Different ACO algorithms have been effectively used in the implementation where a trust relationship is established between different entities in the cloud. The method proposed by the author is ACO-BTM the trust model where pheromone concept and the transition probability are used to represent the mutual trust.

A storage architecture trusted model for storage architecture in the area of cloud computing is proposed by Ullah, et al, 2014,[44] . This architecture presents a very different way to access varied data from the cloud in a safe and secure manner from the cloud data center. The architecture gave a standard set of authorized users

Who have the credentials to access the data from secure storage and accessing of data from cloud data center. The violation of various security parameters can still be addressed in this model due to the encryption of this model. The novel architecture uses multilevel authentication system.

Anagreh, at el, 2014, [45] proposed the Elliptic Curve Cryptography (ECC) optimization algorithm where only one of the ECC calculations needs to be modified. This method is based on the Mutual opposite form algorithm. The algorithm combines both the MOF and add-subtract multiplication algorithm which will help in speeding up the existing ECC scalar multiplication. The implementation shows that the algorithm improves both the computational time and effective speed up which is up to 90% speed-up compared to the existing methods.

The concept of dynamic secret presented by Liu, at el, 2014, [46] where designing smart grid wireless communication is applied. The smart grid platform is built on the Zignee protocol where dynamic encryption demo which is a secret based system is used. The experiment results stated that packet loss and re transmission in ZigBee communication is inevitable where it almost becomes very difficult to track the dynamic key encryption.

Liu, at el, 2014[47] presented an evaluation mechanism between the image encryption optical technique and the chaos theory. Thorough statistical analysis is done by the author where statistical analysis and image robustness are taken into consideration. Both these have their own weakness and strengths thus when both the methods are combined better results can be achieved.

The asymmetric algorithms created by Diffie and Hellman in 1976, used one key for encryption and a separate key for decryption. Followed by DH (Diffie-Hellman) protocol, the researchers in 1977 developed an algorithm called RSA, RSA refers to its discoverers, Rivest, Shamir, and Adleman. With the rapid development of cryptography research and computer technology, the capabilities of various cryptosystems such as of RSA and Diffie-Hellman will prove to be lagging when large data sets or large number of bits are taken into consideration which is discussed by Kapse, et al, 2014, [48].

The size of bits increases the security of the algorithm but if we use the higher bits security then the computational requirements becomes very complicated as well as expensive. The author stated that increasing from a 1,024-bit RSA key to a 2,048-bit key requires as much as eight times of the computational processing. When we use the hand-held products like the PDA and computational devices are taken into consideration this might not be recommended as the processing speed is not sufficient enough. The PDA systems might not have the capability of processing when RSA keys of 3,072 bits and above are used which is proposed in his research study by Brohi, et al, 2014,[49]

A new variant of ACO is proposed by Forsati, et al, 2014,[50] which is called enRiched Ant Colony Optimization (RACO). The author proposed this method in which the previously traversed edges are first executed then it becomes relatively easy to update the pheromone values. The advantage of this method is that it will prevent premature coverage. The proposed method is very effective compared to all previous methods and it provides better path coverage.

A novel method of ACO in which it uses Swarm Intelligence (SI) application techniques in a navigational Decision Support System (DSS) was developed by Lazarowska, et al 2014,[51] . In this path planning, collision avoidance of the ship are developed which can be used in open sea or restricted waters. With the advent of this automated system safe ship control process is achieved to a greater extent.

Sina, et al, 2014, [52] proposed a new method which has low computational complexity, thus it can be applied for high dimensional datasets. The feature relevance will be computed based on the similarity between features, which leads to the minimisation of the redundancy. Therefore, it can be stated that the proposed method by the author which is filter-based method is very effective and efficient compared to the previous existing methods.

Eldem, et al, 2014 ,[53] proposed ACO optimization which is effectively applied to solve Euclidian TSP. The proposed method consists of 9 different varied sets of nodes which are placed on a cuboid surface randomly. The novel method can be applied to real world where the author has already collected the potential samples. Different buildings, glasses, walls, furniture are taken into consideration. The performance evaluation is done with different tests and proved to be very effective.

A comparison of multi-population and single evolutionary algorithm is presented by Smierzchalski, et al, 2014, [54]. The author presented the tested algorithms where the different paths can determine closeness to ship paths and collision avoidance. The path planning where individual and multiple paths along with the fitness function are identified. The presented algorithms have been simulated in the real sea environment. The challenging situation where simulation is performed is when nearing to the sea but constant time simulation is maintained to give better results. All the identified results are presented in different forms to show the effectiveness of the proposed algorithms.

The method for fault routing in ACO when load balancing is done in faulty networks is identified by Kai, et al, 2014, [55]. In the proposed algorithm congestion free paths can be identified and all the available routes are stated which helps in sending the packets through a congestion free path. The experimental results have been carried out with simulation where the throughput increased from 29.1%-66.5% and also the undelivered packet ratio is reduced by 0.5%-0.02%. Thus, the distribution of traffic flow when in the faulty network is also very good and the proposed method can be used effectively.

A recent research study is done by Shaukat, et al, 2014, [56] in which it states that ACO is most preferred way to solve the TSP problem. Ant colony systems were studied which acts as a collection of different ant colony optimization. Best solutions are found by ants which act as a cooperative agent as Ants cooperate with each other and communicate using an indirect way with the help of pheromone which is deposited on the edges on the path. After studying ACS as different ACO techniques are compared so implementation results are also taken.

With the increase of social networking personalized social matching systems can be recommended to people. In this work, ACO based algorithm is proposed to solve the optimisation problem of matching people in different social networks which were designed for this purpose. All the user preferences and personal characters are taken when doing the process. Results proved that clustering can be effectively performed by this proposed algorithm which is recommended by Mendonca, et al, 2014,[57]

Cheng, et al, 2014, [58] proposed his research study on reliability of cloud systems. A definition of reliability of

cloud service system is given on the basis of a detailed approach of the operation of cloud service system, and the development of the overall system reliability mathematical model by phased analytical modeling method is discussed.

Trust Management (TM), in the mutual trust based access control (MTBAC) model is proposed byLin, et al, 2014, [59] . The proposed model takes the credibility of the cloud node and users trust into consideration. The trust relationship has to be established by the mutual trust mechanism. The author states that the security problems of different access control mechanisms in the cloud can be easily sorted when the method is implemented in the real world.

Heilig, et al, 2014, [60] proposed his research study where different and large databases are applied to the scientometric means. The proposed method studies the cloud computing research by taking into consideration different clouds. Different publication patterns and research impacts, productivity is taken into consideration. The results of the study give better trends and patterns which will act as a future direction for research as well as better knowledge sharing in the area of cloud computing research.

Abolfazli, et al, 2014 [61] presented an analysis on different CMA approaches and various mobile augmentation domains. The author classified the different CMA approaches into distant fixed, proximate fixed, proximate mobile, and hybrid to present taxonomy. He introduces a decision-making chart which states the performance limitation details and decision-making issues in the current world.

Kai, et al, 2014, [62] proposed a model for the rate allocation and topology configuration where C-RAN is taken into consideration. The end-to-end performance which is used in different mobile networks is implemented in this model. The Decision theoretical approach which is used to solve the delayed channel information and various other problems in C-RAN are used and the method proves very effective in the current world.

A Framework for the trusted Cloud in the Healthcare Sector is proposed by Adib, et al, 2014, [63]. The author proposes the usage of stringent security controls and also multi-factor authentication access mechanisms. The proposed method covers different application layers and virtualization as well. This method can be effectively used in the healthcare field and it is better than the previous existing methods in this area as the method is also HIPAA complied.

Khan, et al, 2015, [64] proposed his research study on Context-Aware Cloud Computing in mobiles and various Challenges in that area. The author has stated that the development of cloud-enabled applications have the capability to move towards more demands and changing needs in smart phone applications. This can be effectively used by future researchers where mobile based implementations are in picture.

A novel algorithm where digitally signed cipher images which provides authenticity, integrity and security are implemented by ECC was presented by Singh ,et al,2015,[65]. The author considers the Pixel values which play a key in this algorithm where mapping values to elliptical curve was not necessary. He ignored the reference mapping tables thus benefitting from the other existing approaches as low and correlated cipher images were generated in this method.

Thomas, et al, 2015, [66] presented a secure elliptic curve scalar multiplication using Karatsuba multiplier. The comparison is made with classical polynomial multiplier, recursive Karatsuba multiplier and hybrid Karatsuba multiplier. The simulation results show that hybrid Karatsuba multiplier consumes less area than the other two multipliers. The implementation of the elliptic curve multiplication at a point is achieved by using a dedicated Galois Field arithmetic simulated on ModelSim. The research work also includes generating key pair for encryption and decryption in elliptic curve cryptography

A novel task scheduling policy which operates on cloud and uses the ACO algorithm is proposed by Tawfeek, et al, 2015[67]. The author identified few task sets which can considered to implement the problem and the algorithms were implemented where the make span is drastically minimised for the considered task sets. ACO is like an optimisation search approach which will randomly allocate the jobs to the VM. The author applied the cloud task scheduling and compared the same with existing RR and FCFS and results stated that the current algorithm is very efficient compared to the previous existing approaches.

Bahrami et al 2015,[68] proposed his research study in introducing various cloud services for mobiles which will benefit the people who can develop various apps. He analysed how vendors can improve the app business. In experimental results he considers major cloud vendors like Microsoft Windows Azure, Amazon and Google Cloud Platform. The author came up with cutting edge practices in this field, and presented different opportunities for future development.

ECC is extremely computationally efficient algorithm which provides lesser execution time, requires lesser memory, lesser bandwidth, and lesser energy consumption. Hence, ECC is Endorsed by the different agencies like NIST Aguero, et al, 2015,[69] studied the various usages

and future enhancements which will act in an efficient way with the changing needs of the people.

Stackelberg game model is proposed by Yin, et al, 2015, [70]. The author formulated various problems which occur when mobile cloud environments.. The proposed game model is further extended with different players which are in the network and solved the game with available small cells. Backward induction method analysed the proposed Stackelberg game. Simulation results are identified to show the effectiveness of the proposed model.

III METHODOLOGY

The proposed HECC message is coded with the symmetric code and the key over the coded message is encrypted using the asymmetric coding algorithm. The creator will now take the data key and will decode it using the asymmetric coding algorithm to that the recipient's public key. The operation forms a key Block. But the advantage of this is thought it is highly compute intensive the size of the data key which we are taking is very small thus the complete process will be done in just a fraction of second. The creator will collect the data block and the key which was stored as a block into a file and transmits the file to the recipient

The new Hybrid ECC (HECC) has two stages of operation which are explained in the following sub sections:

STAGE 1

At first the originator and the recipient of the data must both agree on the parameters for ECC, that is, the domain parameters of the scheme. The field of domain in ECC is defined by 'p' in the prime case and the pair of 'c' and 'd' in the binary case. The elliptic curve is defined by the constants 'a' and 'b' used in its defining equation. The elliptical curve will now be a plane curve which is simple and spread over finite field. It consists of points which satisfy the equation

$$y^2 = x^3 + ax + b$$

along with a distinguished point at infinity, denoted .

STAGE 2

The Generator G will be defining the Monogenous group that is generated by the single element. There are several logarithm-based protocols that are available, which will restore the (Zp)x with the elliptical curve. Here we are choosing Elliptic curve Diffie –Hellman key agreement scheme based on Diffie Hellman scheme is being used.

For cryptographic application G, which is the smallest non-negative number n so that nG=∞, which in most cases is prime. Since n is the size of a subgroup of E(Fp) from Lagrange's theorem it can be shown that the number h is an integer. The h is expressed in equation

$$h = \frac{|E(F_p)|}{n}$$

In cryptographic applications this number h, which is the cofactor, must be small and preferably h should be 1. Unless and until there is assurance that the parameters are generated by the trusted party they need to be validated before we use them

The generation of domain parameters is not usually done by each participant as this process involves computing the number of points on a curve. This process is computing intensive, time-consuming and troublesome to implement. There are few domain parameters which are already proposed by the standard bodies for several common field sizes to overcome this reason [65]. These domain parameters which are termed as named curves which can be the NIST (National Institute of Standards and Technology) curve.

The above-mentioned algorithms will generate the curve based on the respective fields. But if any user wants to create their own parameters than there are several strategies that are available and mentioned below which can be used to generate the curve with the required set of points on the field:

Firstly, The user can select the random curve and then apply a general point-counting algorithm like Schoof's algorithm or Schoof–Elkies–Atkin algorithm,

Select a random curve in a family of curves like the Koblitz curve can be used or Select the number of points required and then generate a curve with this number

The projected phenomenon can be compared to a finite-field cryptography (e.g., DSA) that will need 3072-bit public keys and 256-bit private keys, and integer factorization cryptography (e.g., RSA) which requires a 3072-bit values of n, Hence, even if the public key is large, the private key which can be small will be used for encryption. With the smaller key size less computation and faster processing will be achieved. Especially smaller processors are present. The method of operation is explained through the following block diagram in Fig.1.

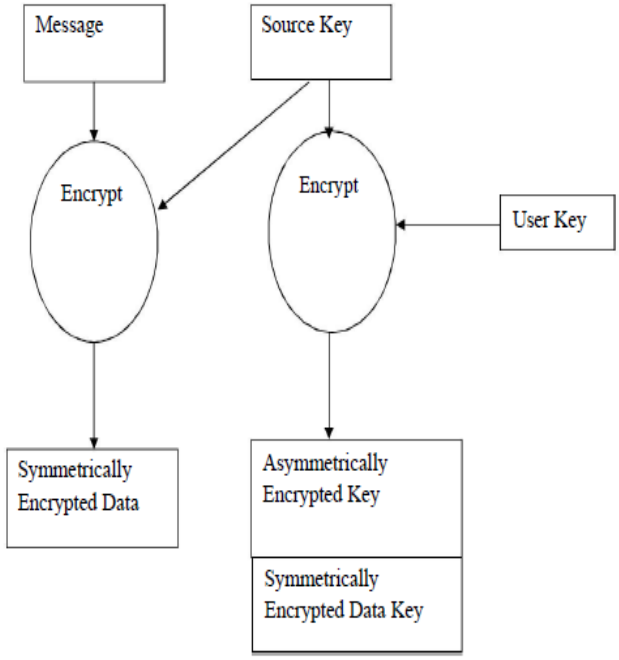

Fig. 1 Proposed hybrid ECC

In the proposed hybrid ECC approach, the data is encrypted using a symmetric algorithm, and then the key to the encrypted data is encrypted using an asymmetrical algorithm. The originator will take the data key and encrypt it using an asymmetric algorithm and the end user's public key. This process is known as a key block. Though the process requires lot of computational effort but still as the key size is itself very small so the time taken will also be a fraction of a second. Finally, the originator bundles the data block and key block into a single file and communicates this file to the end use.

ALGORITHM

Step 1: Begin

Step 2: Initialization: Both sender and receiver must agree on elements of ECC while defining an elliptic curve

Step 3: ECC='p' in Prime case else 'm' and 'f' in case of binary

Step 4: Constants are a and b in defining an elliptic curve

$$y^2 = x^3 + ax + b$$

Step 5: The elliptical curve will be a plane curve which is simple and spread over finite field. It consists of points which satisfy the equation mentioned in step 4

Step 6: For cryptographic application the order of G, that is the smallest non-negative number n such that nG=∞, which is normally prime.

Step 7: n is the size of a subgroup of E(Fp) it follows from Lagrange's theorem that the number h is an integer. The h is expressed in equation:

$$h = \frac{|E(F_P)|}{n}$$

Where (h≤4) and, preferably, h=1

Step 8: So the parameters in prime case are (p, a, b, G, n, h) and in the binary case they are (m, f, a, b, G, n, h).

Step 9: End

IV RESULTS AND DISCUSSION

The proposed work is undertaken in NS2, the famous tool for event networking simulation. Experimental results are taken comparing the memory requirements and execution time of ECC with existing methods. The Fig.3.2 and 3.3 show the comparison of execution time and memory requirements respectively.

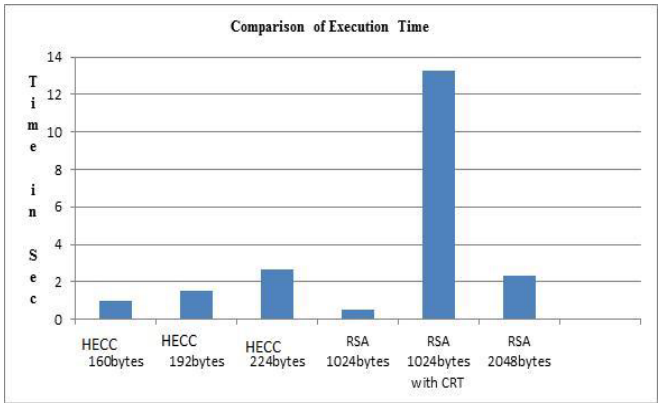

Fig. 2 Performance Comparison of execution time

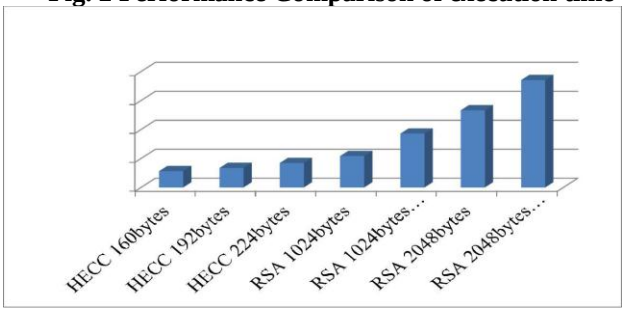

Fig 3.3 Performance comparison of memory requirements

The performance of the proposed algorithm is compared with existing algorithms for the maximum of 200 nodes. The result of various methods based on storage space requirement and time consumption are listed in the table 1 and 2.

Table 1 Storage Space Required (in MB)

No of Nodes	RSA	PKC	RSA-CRT	ECC	HECC

20	273.8	412.3	102.7	93.5	84.1
40	350.46	527.74	126.32	115	103.5
60	448.59	675.51	155.37	141.4	127.2
80	574.2	864.66	191.11	173.9	156.5
100	734.98	1106.8	235.07	213.9	192.5
120	940.77	1416.7	289.13	263.1	236.8
140	1204.2	1813.3	355.63	323.6	291.3
160	1541.4	2321	437.43	398.1	358.3

Table .2 Time Consumption (in ms)

No of Nodes	RSA	PKC	RSA-CRT	ECC	HECC
20	273.8	412.3	102.7	93.5	84.1
40	350.46	527.74	126.32	115	103.5
60	448.59	675.51	155.37	141.4	127.2
80	574.2	864.66	191.11	173.9	156.5
100	734.98	1106.8	235.07	213.9	192.5
120	940.77	1416.7	289.13	263.1	236.8
140	1204.2	1813.3	355.63	323.6	291.3
160	1541.4	2321	437.43	398.1	358.3
180	1972.9	2970.9	538.04	489.6	440.7
200	2525.4	3802.8	661.78	602.2	542

The scalability of the proposed algorithm is also verified through experimental result which is shown in table 3.4; in all existing methods, the time consumption of the concern method is increased much more when number of nodes incremented, whereas in the proposed system it is less than a minute. The time consumption in the mobile and cloud node for key exchange of existing and proposed methodologies are shown in table 3.3 and 3.4.

Table 3 Time Consumption in mobile node for Key Exchange (in bits)

No of Nodes	RSA	PKC	RSA-CRT	ECC	HECC
160	3	4	3	3	2
256	7	11	8	7	7
512	16	18	15	14	12
1024	22	28	19	17	16
2048	166	178	122	111	100

Table. 4 Time Consumption over cloud for key exchange (in bits)

No of Nodes	RSA	PKC	RSA-CRT	ECC	HECC
160	1.2	1.8	1.1	1	0.9
256	4.3	5.2	4.1	3.7	3.3
512	7.4	8.6	7	6.4	5.7
1024	10.4	12	10	9.1	8.2
2048	13.5	15.5	12.9	12	10.6

It is observed from the results, the proposed HECC is giving optimal results with respect to execution time and memory requirements compared to existing methods. The handheld devices approaching cloud will optimally use the proposed HECC for smooth, faster and secured functionalities. There are more challenges in finding optimal solutions in many discrete mathematical problems in the area of engineering domain. The Ant colony optimization (ACO) uses swarm intelligence technique which has been used for finding the solution for the challenges in our research study. The new methodology based on ACO is proposed which is described in detail in the next chapter.

CONCLUSION

The proposed system has two components for providing secured cloud computing, which are Hybrid ECC and ACO based Security Model. The proposed HECC and ant colony-based authentication system is implemented in Azure platform. The performance of the network model is simulated using in NS2. The average end-to-end delay which affects the performance of the system when the values are high and the user will feel the system is hanged. In general, 150ms is a critical value; the existing ACO also performs reasonable value of end-to-end delay. However, the proposed ACO performs well on account of the speed of data transmission The performance of RSA, ECC and the proposed HECC are compared in terms of its execution time, memory requirements in bytes and energy consumption. From the results, it is observed that the performance of proposed HECC having optimal results in terms of key exchange time, space complexity and energy consumption. This novel methodology is successfully implemented in the smart military-based application and the experimental results states that there is no packet loss, even at 100 nodes are transferring data at the time as the proposed military system has cloud resources. And the packet loss on above 100 nodes is also less than 25% of existing military systems. Similarly, the response time of the proposed military system is faster. The data receiving capability of the proposed and existing system is recorded in terms of throughput. The throughput of the proposed military system is always higher than the existing military systems. Hence, it is concluded that the proposed cloud based secured and smart military system is optimal than existing military system.

REFERENCES

[1]. Wang You-Bo, Dong Xiang-Jun, Tian Zhi-Guang. " FPGA Based Design of Elliptic Curve Cryptography Coprocessor", Third International Conference on Natural Computation,vol.5, pp. 185-189,2007

[2]. Jarvinen K., Skytta J. " On Parallelization of High Speed Processors for Elliptic Curve Cryptography", In Proceedings of IEEE International conference on Very Large Scale Integration Systems, vol.16(9),pp.1162-1175,2008

[3]. L.Y. Li and Y. Xiang. "Research of Multi-Path Touting Protocol Based on Parallel Ant Colony Algorithm Optimization in Mobile Ad Hoc Networds", In Proceedings of International Conference on Information Technology,pp.1006-1010, 2008.

[4]. Han L. and Berry D. "Semantic-Supported and Agent Based Decentralized Grid Resource Discovery", Computer Journal of Future Generation Computer Systems, vol. 24(8),pp.806-812, 2008

[5]. Z. Zhang, X. Zhang. "Realization of open cloud computing federation based on mobile agent", In proceedings of IEEE International Conference on Intelligent Computing and Intelligent Systems, vol. 3, pp. 642–646,2009

[6]. Athavale A.; Singh K.; Sood S. "Design of a Private Credentials Scheme Based on Elliptic Curve Cryptography", In proceedings of First International Conference on Computational Intelligence, Communication Systems and Networks, pp. 332-335,2009

[7]. Greenberg, J. Hamilton, D. A. Maltz and P. Patel. "The cost of a cloud: Research problems in data center networks", Computer Commuication Review, vol. 39(1), pp.68 -73,2009

[8]. M. Armbrust. "A view of cloud computing" Journal of the Association for Computing Machinery, vol. 53, pp. 50- 58, 2010

[9]. Pathak H. and Sanghi M. "Speeding-up Computation of Scalar Multiplication in Elliptic Curve Cryptosystem", International Journal on Computer Science and Engineering, vol. 2, pp. 1024-1028, 2010.

[10]. Dinh HT, Lee C, Niyato D, Wang P. "A survey of mobile cloud computing: architecture, applications, and approaches" In Proceedings of the wireless communications and mobile computing,vol.13(8), pp.1587-1611,2011

[11]. Y. Zhang and J. Grobschadl. "Encient prime field arithmetic for elliptic curve cryptography on wireless sensor nodes." In Proceedings of the International Conference on Computer Science and Network Technology , vol. 1, pp. 459-466, 2011

[12]. Chia-Feng Juang, Chun-Ming Lu, Chiang Lo and Chi-Yen Wang. "Ant Colony Optimization Algorithm for Fuzzy Controller Design and Its FPGA Implementation", In proceedings of IEEE international conference on Plasma Science, vol. 39, 2011

[13]. Farah Mourad, Hicham Chehade, Hichem Snoussi, Farouk Yalaoui, Lionel Amodeo, C, Edric Richard. "Controlled Mobility Sensor Networks For Target Tracking Using Ant Colony Optimization", In Proceedings of IEEE International conference On Mobile Computing, vol. 11, pp. 1261 – 1273, 2011

[14]. Hai Ming Jiang, Kang Xie and YaFei Wang. "Novel Design of Flat Gain Spectrum Raman Fiber Amplifiers Based On Ant Colony Optimization", In Proceedings of IEEE International conference on Photonics Technology Letters, vol. 23, 2011

[15]. M. Jarschel, D. Schlosser, S. Scheuring and T. Hobfeld. "An evaluation of QoE in cloud gaming based on subjective tests", In Proceedings of IEEE international conference on innovative mobile and internet services in Ubiquitous Computing, pp. 330-335, 2011

[16]. Mahamat Hassan. and Azween A. "A New Grid Resource Discovery Framework", The International Arab Journal of Information Technology, vol. 8(1),pp. 99-107, 2011

[17]. X. W. Zhang, A. Kunjithapatham, S. Jeong and S. Gibbs. "Towards an elastic application model for augmenting the computing capabilities of mobile devices with cloud computing", Mobile Networks & Applications, vol. 16(3), pp.270 -284,2011

[18]. LiLi, Ahmed A. Abd El-Latif and XiamuNiu. "Elliptic Curve ElGamal Based Homomorphic Image Encryption Scheme for Sharing Secret Images in Signal Processing", Elsevier, vol. 92, pp. 1069–1078, 2012

[19]. S. Maria Celestin Vigila and K. Muneeswaran. "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications", International Journal of Network Security , vol. 14(4), pp. 236–242, 2012

[20]. Loai Tawalbeh, Moad Mowafi and Walid Aljoby. "Use of Elliptic Curve Cryptography for Multimedia Encryption", IET Information Security ,vol. 7(2), pp. 67–74, 2012

[21]. S. Barber, X. Boyen, E. Shi, and E. Uzun. "Bitter to better - how to make bitcoin a better currency" ,Lecture Notes in Computer Science- Springer ,vol. 7397, pp. 399-414, 2012

[22]. Bai Qing-hai; Zhang Wen-bo; Jiang Peng; Lu Xu. "Research on Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation", International Conference on Computer Science and Service System, pp. 1224-1227,2012.

[23]. Y. Volkan Pehlivanoglu "A new vibrational genetic algorithm enhanced with a Voronoi diagram for path planning of autonomous UAV", Aerospace Science and Technology, vol. 16, pp. 47-55, 2012.

[24]. Ratan Mishral, and Anant Jaiswal. "Ant colony Optimization: A Solution of Load balancing in Cloud", International Journal of Web & Semantic Technology,vol. 3(2), 2012.

[25]. S.Dey. "Cloud mobile media: Opportunities, challenges, and directions",In proceedings of International conference on Computing, networking and communications, pp.929 -933, 2012

[26]. R. Kokku, R. Mahindra, H. Zhang and S. Rangarajan. "NVS: A substrate for virtualizing wireless resources in cellular networks", In Proceedings of IEEE International conference, vol. 20(5), pp.1333 -1346, 2012

[27]. Gao Y., Guan H., Qi Z., Hou Y., and Liu L, "A Multi-Objective Ant Colony System Algorithm for Virtual Machine Placement in Cloud Computing", Journal of Computer and System Sciences, vol. 79(8), pp. 1230-1242, 2013.

[28]. S. F. Abbas. "Metric Base Analysis and Modeling Experiments of Routing Protocols in MANETs and VANETs Wireless Network using Real Time Scenarios", International Journal of Computer Science Issues, vol. 10(5),2013.

[29]. Niroshinie Fernando,Seng W.Loke,Wenny Rahayu. "Mobile cloud computing: A survey", Future Generation Computer Systems, vol.29 ,pp.84–106,2013

[30]. A. Ahmed, Abd El-Latif and XiamuNiu."A Hybrid Chaotic System and Cyclic Elliptic Curve for Image Encryption",International Journal of Electronics and Communications, Elsevier, vol. 67, pp. 136–143, 2013

[31]. H. Seo and H. Kim. "Optimized multi-precision multiplication for public-key cryptography on embedded microprocessors", International Journal of Computer and Communication Engineering , vol. 2,pp. 255-259, 2013

[32]. Arshad R, Ikram N."Elliptic curve cryptography based mutual authentication scheme for session initiation protocol", Multimedia Tools and applications, vol. 66(2), pp. 165–178,2013

[33]. Ali Soleymani, Md Jan Nordin and Zulkarnain Md Ali. "A Novel Public Key Encryption based on Elliptic Curves Over

Prime Group Field", Journal of Image and Graphics , vol. 1, pp. 43–49, 2013
[34]. S. Behnia, A. Akhavan, A. Akhshani and A. Samsudin. "Image Encryption based on the Jacobian Elliptic Maps", The Journal of System and Software, Elsevier, vol. 86, pp. 2429–2438, 2013
[35]. Irshad A, Sher M, Faisal MS, Ghani A, Ul Hassan M, Ashraf Ch S. " A secure authentication scheme for session initiation protocol by using ECC on the basis of the Tang and Liu scheme", Security and communication Networks, vol. 7(8),pp. 1210–1218,2013
[36]. Sharma G, Bala S, Verma AK. "An identity-based ring signcryption scheme", IT convergence and security, Springer, pp151–157,2013
[37]. Y., Wang, G., Chen, H., Shi, L., Qin, L. "An ant colony optimization based dimension reduction method for high-dimensional datasets",Journal of Biological Engineering, vol. 10,pp. 231–241,2013
[38]. Baig, A.R.; Shahzad, W.; Khan, S. " Correlation as a Heuristic for Accurate and Comprehensible Ant Colony Optimization Based Classifiers" In Proceedings of IEEE International conference on Evolutionary Computation, vol. 17(5),pp. 686 - 704,2013
[39]. Wei-Neng Chen; Jun Zhang , "Ant Colony Optimization for Software Project Scheduling and Staffing with an Event-Based Scheduler", In Proceedings of IEEE International conference on Software Engineering,vol 39(1),pp. 1 – 17,2013
[40]. Zhanchang Yu, Sijia Zhang, Siyong Chen, Bingxing Liu, Shiqi Ye. "Research on Traveling Routes Problems Based on Improved Ant Colony Algorithm", Communications and Network, vol. 5, pp. 606-610,2013
[41]. Lie Qu,Yan Wang,Mehmet A Orgun. "Cloud Service Selection Based on the Aggregation of User Feedback and Quantitative Performance Assessment", In proceedings of IEEE international conference on services compurting, pp.152-159,2013.
[42]. Ijaz S., Munir E., Anwar W., and Nasir W. "Efficient Scheduling Strategy for Task Graphs in Heterogeneous Computing Environment", The International Arab Journal of Information Technology, vol. 10(5), pp. 486-492, 2013
[43]. Guoyuan Linabd, Yuyu Biea, Min Leic, Kangfeng Zhengc. "A Behavior Trust Model in Cloud Computing Environment" International Journal of Computational Intelligence Systems, vol. 7(4), pp.785-795, 2014
[44]. Sultan Ullah, Zheng Xuefeng. "TCLOUD: A Trusted Storage Architecture for Cloud Computing" International Journal of Advanced Science and Technology, vol.63, pp.65-72, 2014
[45]. Mohammad Anagreh, AzmanSamsudin and MohdAdib Omar. " Parallel Method for Computing Elliptic Curve Scalar Multiplication Based on MOF", The International Arab Journal of Information Technology, vol. 11, pp. 521-525, 2014
[46]. Ting Liu, YangLiu, YashanMao, Yao Sun, XiaohongGuan, Weibo Gong, Sheng Xiao "A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication" In Proceedings of IEEE International conference on Trans Smart Grid, vol. 5(3), 2014
[47]. Hong Liu and Yanbing Liu. "Cryptanalyzing an Image Encryption Scheme based on Hybrid Chaotic System and Cyclic Elliptic Curve,In Optics and Laser Technology" , Elsevier, vol. 56, pp. 15–19, 2014
[48]. Akshay D. Kapse, Piyush K. Ingole"Secure and Efficient Search Technique in Cloud Computing", In Proceedings of IEEE International conference on Communication systems and network technologies, pp.743-747,2014
[49]. Brohi S.N.. M.A. Bamiah, S. Chuprat and J.L.A. Manan. "Design and implementation of a privacy preserved off-premises cloud storage", Journal of Computer science, vol.10,pp. 210-223,2014
[50]. R. Forsati, A. Moayedikia, R. Jensen, M. Shamsfard and M. R. Meybodi. "Enriched ant colony optimization and its application in feature selection", Neurocomputing, vol. 142, pp.354 -371, 2014
[51]. Agnieszka Lazarowska. "Ant Colony Optimization based navigational decision support system", Procedia Computer Science, vol. 35,pp 1013– 1022,2014
[52]. Tabakhi Sina, Parham Moradi and Fardin Akhlaghian. "An unsupervised feature selection algorithm based on ant colony optimization", Engineering Applications of Artificial Intelligence, vol. 32, pp.112 -123, 2014
[53]. Huseyin Eldem, Erkan Ulker. "Application of Ant Colony Optimization for the Solution of 3 Dimensional Cuboid Structures", Journal of Computer and Communications, vol. 2, pp. 99-107,2014
[54]. Smierzchalski R, Kuczkowski L. "Comparison of single and multi-population evolutionary algorithm for path planning in navigation situation",ultra clean processing of silicon surfaces, vol. 210,pp.166-177,2014
[55]. Hsien-Kai Hsin; En-Jui Chang; Chia-An Lin; Wu, A.-Y.A. "Ant Colony Optimization-Based Fault-Aware Routing in Mesh-Based Network-on-Chip Systems", Computer-Aided Design of Integrated Circuits and Systems, vol. 33(11), pp.1693-1705,2014
[56]. Sundus Shaukat, Riaz Ahmed Bhatti, Khalid Ibrahim Qureshi and Shafqat Ali Shad, "Ant Colony Optimization: A Review and Comparison" Research Journal of Applied Sciences, Engineering and Technology,vol.8(3),pp. 435-438, 2014
[57]. Luziane Ferreira de Mendonca. "An Approach for Personalized Social Matching Systems by Using Ant Colony" ,Social Networking, vol. 3,pp 102-107,2014
[58]. Bing quan Cheng "Cloud Service System Reliability Modeling, Electronic Product Reliability and Environment Testing", vol. 32(2), pp.22 -27, 2014
[59]. Guoyuan Lin; Danru Wang; YuyuBie; Min Lei "MTBAC: A mutual trust based access control model in Cloud computing", In Proceedings of IEEE International conference ,vol. 11(4),pp.154 – 162,2014
[60]. Heilig, L.; Vob, S. "A Scientometric Analysis of Cloud Computing Literature" , In Proceedings of IEEE International conference on Cloud Computing, vol. 2(3),2014
[61]. S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani and R. Buyya. "Cloud-based augmentation for mobile devices: Motivation, taxonomies, and open challenges", In Proceedings of IEEE International conference ,vol. 16(1), pp.337 -368, 2014
[62]. Y. Cai, F. R. Yu and S. Bu. "Cloud computing meets mobile wireless communications in next generation cellular networks", In Proceedings of IEEE International conference ,vol. 28(6), pp.54 -59, 2014
[63]. Bamiah, Mervat Adib; Brohi, Sarfraz Nawaz; Chuprat, Suriayati& 2Jamalul-lail Ab Manan. "Trusted Cloud Computing Framework For Healthcare Sector", Journal of Computer Science, vol. 10(2),pp. 240-250,2014
[64]. Atta ur Rehman Khan, Mazliza Othman ,Feng Xia ,Abdul Nasir Khan, "Context-Aware Mobile Cloud Computing and Its Challenges", In Proceedings of IEEE International conference on Cloud Computing, vol. 2(3),pp. 42-49,2015
[65]. Laiphrakpam Dolendro Singh and KhumanthemManglem Singh. "Image Encryption using Elliptic Curve Cryptography", Procedia Computer Science, vol 54,pp. 472-481,2015
[66]. Christina Thomas ,Gnana Sheela K , Saranya P Krishnan. "An Efficient Elliptic Curve Scalar Multiplication using Karatsuba Multiplier", International Journal of Engineering Research and General Science, vol. 3, pp. 1074-1086,2015

[67]. Medhat Tawfeek, Ashraf El-Sisi, ArabiKeshk and FawzyTorkey. "Cloud Task Scheduling Based on Ant Colony Optimization", The International Arab Journal of Information Technology, vol. 12(2), March 2015
[68]. Mehdi Bahrami. "Cloud Computing for Emerging Mobile Cloud Apps" In proceedings of IEEE international conference, pp. 4-5,2015
[69]. C. Aguero, N. Koenig, I. Chen, H. Boyer, S. Peters, J. Hsu, B. Gerkey, S. Paepcke, J. Rivero, J. Manzo, E. Krotkov, and G. Pratt. "Inside the Virtual Robotics Challenge: Simulating Real-time Robotic Disaster Response", In Proceedings of IEEE International conference on Automation Science and Engineering ,vol. 12(2), 2015.
[70]. Zhiyuan Yin; Yu, F.R.; Shengrong Bu; Zhu Han. "Joint Cloud and Wireless Networks Operations in Mobile Cloud Computing Environments With Telecom Operator Cloud" In Proceedings of IEEE International conference on Wireless Communications,vol.14(7), pp.4020-4033,2015
[71]. Brown, Michael, et al. Software implementation of the NIST elliptic curves over prime fields. Springer Berlin Heidelberg, 2001.
[72]. Cohen, Henri, Atsuko Miyaji, and Takatoshi Ono. "Efficient elliptic curve exponentiation using mixed coordinates." Advances in Cryptology—ASIACRYPT'98. Springer Berlin Heidelberg, 1998

Authors Profile

P. Madhubala pursued Ph.D. in Computer Science from Mother Teresa Women's University, kodaikanal in the year 2017. She is currently working as Head & Assistant Professor in PG & Research Department of Computer Science, Don Bosco College, Periyar University, Salem since 2007. She has published more than 13 research papers in reputed international journals and participated in conferences including IEEE and it's also available online. Her main research work focuses on Cloud Security and Privacy, Cryptography Algorithms, Network Security, and Big Data Analytics. She has 17 years of teaching experience and 5 years of Research Experience.

G.Sakthivrel pursued Bachelor of Science from Sacred Heart College, Madras University, Master of Computer Science from Thiruvalluvar University and M.phil of computer science in the year 2009. He is currently pursuing Ph.D. and working as Assistant Professor in PG Department of Computer Science, Arignar Anna College (Arts & Science) since 2010. He has published more than 3 research papers in reputed international journals and presented papers in National and International conferences. His main research work focuses on Set containment Joins, Cryptography Algorithms, Big Data Analytics and Data Mining. He has 10 years of teaching experience 2 years of Research Experience.

