A Generator Based Polynomial with Secret Encryption Scheme for Secure Data Sharing and Privacy in Multi-Party/Federated-Cloud Computation

V. Keerthi, T. Anuradha

***Abstract:** Now a days exploring and analyzing or mining data in various ways give insights into future for invention and plays a critical role in decision making. For accurate analytical assertion of data, accurate results is essential. So hiding data and at the same time preserving data privacy is necessary to protect externals from attacks. An successful process for sharing sensitive information for data processing, validation and publication should then be deducted. In this paper Polynomial Based Encryption Secret Sharing Scheme (PBESSS) for Multi-Party mechanism is proposed that allows multiple parties to exchange secret data between them at the same time secret data is encrypted so as to protect from untrusted parties. Each party will have stronger protection by selected own polynomial with primitive root number 'generator' and the secret data will be in cryptic form and it can be found by each party after final computation of polynomials. This multi-party mechanism can be applied to federated cloud for computation securely.*

***Keywords:** Multi-Party computation-secret data sharing scheme-polynomial- Galois-Field-cloud-federation.*

I. INTRODUCTION

Local network, broadband internet and/or cloud computing are facing big issue of securing data as it becomes a big concern in certain environments, i.e., if a single copy of the data is stored there is a Possibility of data loss which becomes Data cannot be restored if the copy is lost and it is maintained at single server. The better solution is to have A lot of computer clones which Might boost reliability. Life of data at multiple locations pose security risks and it gives the attackers more opportunities . Also the new Technologies provide a modern way to capture, archive, disseminate and process data, which will help society in terms of information sharing and better use of it by Cooperative estimation of multiple organizations or persons. Via shared computing, owners of separate data wish to combine their tools, without revealing their own data, thereby gaining more useful information and paving the path to stable multi-party computing. Stable multiparty protocol computation [4] Multiple parties are allowed to Compute their input function at the same time maintain the input privacy and the performance accuracy . SMC (Secure Multiparty Computation) is designed so as to prevent an dishonest participant who is corrupt and can get result as that of remaining participants achieve by attacking one of the trusted party. Corrupted players should not be able to discover hidden knowledge about the remaining inputs outside the function's output. Multi-Party computation is applied to latest cloud computation like federated cloud.

In federation of cloud computing where multiple clients residing at different cloud service providers will have to communicate by using the multi-cloud communication mechanism which is proposed in this paper. The security in cloud is an important issue as lots of data is stored at different data centres and is shared across the different clients at different clouds. Therefore a better technology better technology both data availability and confidentiality need to be improved. Therefore, the need for a better technique to enhance both the availability and the confidentiality at data centres encourages the use of secret sharing initiatives [1]. Buyya et al. in [2] proposes an ecosystem named InterCloud that offers cloud-based, just-in-time, opportunistic, and elastic applications services. This suggests the cloud application service (SaaS) providers would find it impossible to fulfil all their customers' QoS standards. Therefore they would prefer to use the resources of various suppliers of Cloud computing that can help support their unique needs. In companies with multinational activities and technologies Online connectivity, media hosting and Web 2.0 software, these types of requisites also emerge. This calls for the creation of frameworks for the federation of cloud infrastructure providers to deliver services seamlessly across various cloud providers[3]. In case of Federated clouds upon exchange of secret data between the Agriculture institutions a secure and effective privacy preserving scheme will be modeled and developed where data is securely shared without loss of information, only data relevant to user is only available for calculation or mining , classification, clustering, associative classification, outsourcing, distributed across various platforms. To perform calculation data to be retrieved by applications and in order to minimize the risk of privacy abuse and to guarantee data confidentiality, confidential data can be exchanged, so secure data exchange systems are necessary. In this article, therefore,

Revised Manuscript Received on December 30, 2020.
***** Correspondence Author

Mrs. V. Keerthi*, Master of Computer Science from Sri Venkateswara University, Tirupathi.

Prof. T. Anuradha, Master of Computer Applications from Sri Padmavathi Mahila Viswa Vidyalayam, Tirupati.

a new data sharing scheme which used generator from Galois field to construct polynomial and securing a secret data is proposed which provides a privacy in data sharing in multi-party computation which is extend to Federated clouds that have multiple host services, ensuring data security and usability.

II. RELATIVE STUDY

In Cryptography, secret sharing will ensure protection of Important material, such as encryption keys. Secret central value is allocated to a variety of pieces — shares — which are pooled to access the initial value. These acts are distributed to separate parties which uses hardware storage methods to protect the key, but the disadvantage of this approach is the need for a large number of expensive hardware. The technique of In modern cryptography, hidden sharing is used to reduce the dangers involved with data that are compromised. Shamir[8] and Blakley[7] suggested secret sharing schemes which provides solution in case of sharing a secret when there is a risk in compromising the value across several parties. In this schemes some security assumptions of sharing a secret is stated if an enemy has access to any number of shares below a certain level, he can not acquire information on the hidden value.

Definition : Let the confidential knowledge be a value s. A T algorithm determines a hidden sharing mechanism k-out-of-n threshold when computing S(s) = [s1, . . . , s_n] and always Correctness and Privacy conditions hold [7,9].

If share s is distributed as individual shares and taken from Secret exchange in a multiparty can be seen computing environment is reliable.

In truth, the protocol is quick and clear as one party (Trusted Party) sends values to other parties in the scheme from a uniform distribution.

This implies that the trusted third party F would not yield anything in the perfect universe. The simulator is simple to construct – only the uniform distribution produces a value and moves it to the opponent. Again the ideals are the same and the opponent cannot discriminate between them.

In paper [1] a technique which will allow file sharing by converting file type as input and data into ASCII strings by using BASE 64 encode scheme is proposed. A set of n shares from ASCII string, is created and distributed one per cloud/location.

The shares are created such that the strings are regenerated by choosing any t shares out of n shares (where t <= n). In this paper file is shared and not the computation, but should be implemented as a separate service, also huge data in terms of trillions of data bytes are to be encoded and decoded each day using base64 which may have performance related issues. Differential privacy on sensitive datasets is proposed in [11]For stable cloud federation data sharing.

A block chain solution is built that allows data owners to control the process of anonymization and to increase service protection. .

It addresses privacy concerns and in case of multi-query scenarios and in case of data sharing by n clients residing at different cloud providers in federation.

By studying above algorithm SMC based mechanism by enhancing security features in the mechanism and it can be applied to cloud entities in federation of cloud.

III. MATHEMATICAL FOUNDATIONS

Number theory, Group theory, Field theory, Galois field, Polynomial computations over fields and the concepts like Primitive Number root and discrete logarithm problem forms the basis for the design of any secure communication scheme. Hence, in the design of secure data sharing scheme following theories and concepts were studied.

Galois Field, named after the finite field, Evariste Galois, refers to an area with a finite number of elements. It is particularly useful in machine translation because it is expressed in binary forms. This implies the machine data consist of two numbers, 0 and 1, the components of the Galois field, which have two elements. The presentation of data as a vector in a Galois field makes it simple and efficient for mathematical operations to scratch data.[12] .

The elements of Galois Field **gf(p^n)** is defined as $gf(p^n) = (0, 1, 2, . . . , p - 1) \cup (p, p + 1, p + 2, . . . , p + p - 1) \cup (p^2, p^2 + 1, p^2 + 2, . . . , p^2 + p - 1) \cup . . . \cup (p^{n-1}, p^{n-1} + 1, p^{n-1} + 2, . . . , p^{n-1} + p - 1)$ where $p \in P$ and $n \in Z+$. The field order is given by pn, while p is called the field characteristic. In the other side, gf, as Galois Field stands. The polynomial degree of each factor is as large as n − 1. A finite order field pn can be represented by GF(p^n) or by gf(p^n).(Note: if not displayed) addition and multiplication modulus of the prime p number is a finite field. The order in the sector is p1. But modulo arithmetic alone will not allow us to construct a finite field for n>1 on order of p^n. The polynomial base is one way of constructing a finite m>1 field. The sector is a series of advances p^m Two polynomial operations polynomials[5,6].

A polynomial f(x) here is a mathematical equation $a_nx^n + a_{n-1}x^{n-1} + ... + a_0$. The highest exponent of x is the polynomial degree . In a polynomial, $a_n, a_{n-1}, ... , a_0$ are called coefficients. If in a polynomial, the coefficients $a_n, a_{n-1}, ... , a_1$ are all 0, or in other words, the polynomial is in the form of a_0, we call this polynomial a **constant**. Polynomial built with coefficients from GF is a primitive polynomial. As with integers, modular arithmetic can be done Polynomials over a field. Now the module and operands are polynomials. In this work polynomial with coefficients are chosen from Galois field as it is constructed with primitive elements[5].

IV. SHAMIR'S SECRET SHARING SCHEME

The secret sharing scheme Shamir[8] is based on polynomial assessments. The key component of the scheme is the trustworthy broker who carries out share estimates of input secrets and distributes to other groups the resulting shares. If the secret is rebuilt, the parties give the broker their stock, who will then merge the shares to get the secret. Shamir's Information Exchange is complex, since it helps a secret owner to safely change the laws of a single secret. That means that a person with a secret may use their position as the secret owner to generate more splits and spread them to more participants if he or she so chooses. Or the secret owner may delete certain participants remotely while the other participants remained totally untouched by the secret sharing scheme. (b) The Shamir scheme is cryptanalytically unbreakable in its encryption paradigm maintaining anonymity so that no shareholder can reveal mutual confidentiality, without first having access to the Hidden Shares threshold number. The secrecy of the scheme members would be kept safe and confidential. The initial data from deconstruction and restoration of the data is only available to the hidden sharer. The Shamir secret exchange scheme[8] is based on polynomial evaluations.

The core element of the scheme is the trustworthy dealer who completes share calculations on input secrets and distributes the resulting shares to other parties. The parties send their shares to the broker as the secret has to be reconstructed, who then will merge the shares and recover the secret. Shamir's Information Exchange is complex, since it helps a secret owner to safely change the laws of a single secret. This means that a person with a secret may use his or her status as a secret owner to generate further splits of a key, and allocate those to more participants if he or she wishes. Or the secret proprietor may delete certain participants manually — leaving the other participants entirely unimpacted in the secret sharing framework. b) The Shamir method is encrypted and cryptanalytical in its cryption model to guarantee a confidentiality that no shareholder will disclose a common secret without first having access to the secret shares threshold number. The secrecy of members in the scheme is kept safe and confidential. The initial data from deconstruction and restoration of the data was only available to the hidden party. Shares in Shamir's scheme are randomly generated polynomial tests by the trusted authority. The polynomial f is generated such that the f(0) assessment exposes the hidden value. If adequate tests take place, the parties may reconstruct the polynomial and measure the secret. Algorithm 1 explains how shares of Shamir's scheme are computed.

a)Algorithm 1: Computation of shares for Shamir's scheme

Data: Finite Field F, secret data s Є F, threshold k, number of shares n

Result: shares $s_1,\ldots, s_n$

Set $f_0 = s$

Uniformly generate coefficients $a_1,\ldots, a_{k-1}$ Є F

Construct the polynomial

$f(x) = a_0 + a_1x + \ldots + a_{k-1}x^{k-1}$

Evaluate the polynomial: $s_i = f(i)$, $(i = 1,\ldots, n)$

Since s=f(0) The index of the shares is The Secret Wert in the algorithm above. S1,........, sn can be traded with their holders for the respective securities. If we need The initial meaning that should be returned, We need at least a subset of k shares. Note that index I and share si have to be stored because it is later needed to rebuild the hidden value.

The classical Shamir algorithm reconstructs the whole Polynomial, while we define only hidden variants f(0) = s. If Shamir's shares are determined, algorithm 2 will recover the confidential value s.

b) Algorithm-2:Share reconstruct for Shamir's scheme

Data: Finite Field F, shares $s_{t1},\ldots, s_{tk}$ Є F where t_j Є {1…..n}are distinct indices

Result: secret data s

calculate reconstruction coefficients β_i by equation (R) above.

compute $f(0) = s_{t1}\beta_{t1} + \ldots + s_{tk}\beta_{tk}$

Return s = f(0)

c. Secret Sharing Scheme Vulnerabilities

According to Tieng, Deneisha Gayle & Nocon, Ederlina[10] three types of attacks that can be done on a secret sharing scheme:

1. **Type 1 attack**: The scammers of both kinds may be trustworthy shareholders who unintentionally show their shares in error or deceptive shareholders who present their counterfeit shares without any cooperation. Each fake part of this attack is a random integer and is entirely independent of other shares.

2. **Type 2 attack:** Cheaters of this sort are dishonest shareholders that deliberately change their shares to trick truthful shareholders. Only if the number of cheaters is higher or equal to the threshold value will cheaters effectively target honest shareholders.

V. PROPOSED POLYNOMIAL BASED ENCRYPTION SECRET SHARING SCHEME (PBESSS)

To overcome above attacks in this thesis Polynomial Based Encryption Secret Sharing Scheme is proposed. In our proposed scheme where one party in sharing mechanism acts as Trusted Authority (TA) which controls the entire computer system and coordinates it. TA will start the protected Scheme for data sharing supplying secret keys and launching the operation. It's built on Shamir's Trusted Authority(TA) this will monitor the whole computation and organize it. TA begins the protected data sharing method by supplying hidden keys and initiating the procedure. It is based on Shamir's (k,n) threshold data sharing scheme and multi-party secure computation mechanism. The proposed PBESSS data sharing scheme is designed and is suitable for federation cloud computing where different clients will participate in computation. This scheme is more secure since each party generates own polynomial based on generator g_i which is secret to each party participating in computation also the secret is encrypted and will be verified at the verification phase. Each polynomial is constructed using coefficients from Field Galois (GF) composed of primitive group elements Z_{Npi}^* created from generator $g_{i..}$

The data exchange mechanism operates in subsequent phases

1. Initialization Phase
2. Distribution Phase
3. Verification Phase
4. Recovery Phase

1. Initialization Phase

In this point, TA will begin a session and session ids will be secretly sent to all parties involved in the computation process. Then TA uses its certificates and sends private and public keys for parties interested in calculations

1. The credentials of each party Pi are sent to TA as P1,P2….Pn
2. TA generates large primes PR_i from credentials of each party Pi.
3. TA computes $NP_i=2*PR_i$
4. For each party Pi, TA generates a primitive root 'g_i' from NPi.
5. TA sends g_i securely which is private to each party Pi, and NPi is public to all the participants(parties).
6. Each party Pi generates a group ZN_{pi}^* with the generator g_i and Npi.

7. P_i builds Galois field (GF) consisting of primitive elements with the group Z_{Npi}^* i.e.,Galois field (ie.,GF(g_i^{bi}) has Φ(gi^{bi} – 1) primitive elements where bi Є Z_{Npi}*.

8. Each party Pi generates a polynomial $h_i(x)$ with coefficients in GF and hence $H_i(x)$ is a GF-Primitive polynomial. [ie. $H_i(x) = a_0x+ a_1x^1+ a_2x^2+\dots\dots\dots+a_{n-1}x^{n-1}$] where

$H_i(0)=a_0$ is the secret value to be shared.

9. Message Digest of the secret value is sent to all parties for verification of its integrity after recovery of secret.

2. Distribution Phase

In this phase each party in group (participants of secret sharing)Exchange computing secrets to obtain the final secret-value polynomial in encrypted form.

1. Each Coefficient a_i in primitive polynomial $H_i(x)$ is the primitive number in GF(g_i^{bi}) where $0<i\leq n-1$ and a_0 is secret value of each party Pi.

2. Each Pi computes, $a_0= S_id_i$ where di=$(g_i^{bi})\delta_i$ where δ_i Є Z_{Npi}* such that $g_i^{bi}\delta_i\equiv 1 \bmod N_{pi}$ here S_i is the secret that is to be shared between parties during computation.

3. Each Pi Group implements Stable Multiparty Computation (SMC) and calculates a polynomial sum.

H(x)= $\sum_{i=1}^{n} hi(x)$and coefficients are in GF sends it to TA for verification.

3. Verification Phase

In this step each group (participant) verifies the hidden value by decrypting and detects the malicious host if they exist and report or deny their value to the Trusted Authority (TA). Any polynomial H(x) with GF(P) coefficient meets the identity , $H(x^P)\equiv[h(x)]^P$

(since g_i=P and GF(P)=GF(g_i)) .

1. TA randomly selects a prime g_{pi} that satisfies the identity stated above. hence $F(x^{gpi})\equiv F(x)^{gpi}$

2. Then TA chooses a small random number t_i Є Z+. ∀ t_i ∃ q_i Є Z+ ∋ $q_it_i\equiv 1 \pmod{g_{pi}}$.

3. TA sends g_{pi}, qi,ti to the corresponding parties Pi and announces as public to all the parties.

4. Each party Pi chooses a secret element r_i∈GF(gi^{bi}) such that $X_{ri}\equiv q_i$(mod H(x), g_{pi})

5. Each party Pi verifies Pj as $X_{ri}{}^{tj}\equiv(Xri)^{tj}\equiv qj^{tj}\equiv 1$(mod (H(x),gpj))

6. If any party Pi is malicious then the above congruence dissatisfies, since the Sum Polynomial H(x) sent from Pi to Pj is wrong.

ie. $X_{ri}{}^{tj} \neq 1$(mod H(x),gpi)

4. Recovery Phase

In this stage after each party has checked Pi, the secret is retrieved by any party using the following steps.

1. Confidentiality can be restored even though a bad entity occurs m(m<n/2).

2.$S=\Sigma(S_id_i)$ where $d_i=(g^{bi})\delta_i$ where δ_i Є Z_{npi}^* such that $g_i^{bi}\ \delta i\equiv 1 \bmod n_{pi}$

3.$S = S_1(g_1^{b1})\delta_1+S_2(g_2^{b2})\delta_2+\dots\dots\dots+S_n(g_n^{bn})\delta_n$.

$S_1g_1^{b1}.\delta_1+S_2g_2^{b2}.\delta_2+\dots\dots\dots+S_ng_n^{bn}.\delta_n$

$=S_1(g_1^{b1}* g_1^{-b1} \bmod np_1)+ S_2(g_2^{b2}* g_2^{-b2} \bmod np_2)+\dots\dots+ S_n(g_n^{bn}* g_n^{-bn} \bmod np_n)$

$= S_1 (g_1^0 \bmod np_1)+ S_2 (g_2^0 \bmod np_2) +\dots\dots\dots+ S_n (g_n^0 \bmod np_n)$

$= S_1*1+ S_2*1+\dots\dots\dots+ S_n*1$

$= S1+S2+\dots\dots\dots+Sn$

4.Secret S is verified with Message digest sent by TA to each party to check whether the Secret S is correct or modified or any fault in computation, so that integrity is maintained.

SMC can be extended to the following three hidden recovery scenarios in the recovery process further where there is a malicious cloud host during data sharing or data recovery when transmitted between different parties.

The proposed scheme is evaluated: a)when all parties participating in computation are honest, b) n-1 participants are honest with some are malicious so for 'n-1' honest parties, in that case among 'n' participants the 'n-1' participants The number of hidden shares is collected as a sum of secret shares. c) that there are malicious parties greater than n/2 among the n participants and secret is calculated. The proposed scheme is used with 'n' number of clouds participating in federation. By allowing parties or clients residing in CSP , Cloud-based PBESSS is an alternate but efficient solution to make generic SMC protocols feasible and scalable to safely outsource their calculations to a cloud provider.

VI. RESULTS AND ANALYSIS

The results are computed by running Java program on I5 processor with 8 GB RAM and the following results are given on Eclipse IDE.

```
INPUTS:Number of Parties involve in the Communication : 3
 Enter long N Value... for party -1  98901
Key Generation Phase:
Cp = 98909
n = 197818
Public  key np : 1 = 197818
Private generator g 1 = 197807
 long N Value... for party -2 89765
Key Generation Phase:
Cp = 89767
n = 179534
Public key np : 2 = 179534
Private generator g 2 = 179527
 long N Value...for party -3  78903
Key Generation Phase:
Cp = 78919
n = 157838
Public key np : 3 = 157838
Private generator g 3 = 157823
170823
  (8)X^2  +  (10)X^1  +  (341646)X^0
  (11)X^2  +  (3)X^1  +  (683292)X^0
  (18)X^2  +  (6)X^1  +  (1024938)X^0
```

The secrets are encrypted above shown as coefficients of X^0

```
The publicly known random variables are ::
{ 3, 5, 7}, The Shares at each Party are ::
P1       P2       P3
q1(3)=341748 q1(5)=341896 q1(7)=342108
q2(3)=683400 q2(5)=683582 q2(7)=683852
q3(3)=1025118   q3(5)=1025418   q3(7)=1025862
The Intermediate Results at each Party are ::
    P1          P2                P3
    2050266    2050266    2050266
    2050896    2050896    2050896
    2051822    2051822
    2051822
```

The Polynomials generated from Intermediate Results and Random values at each party are ::

9a+3b+1c+d = 2050266
25a+5b+1c+d = 2050896
49a+7b+1c+d = 2051822

Each group receives the sum of the polynomials

(37)X^2 + (19)X^1 + (2049876)X^0

Every group decrypts the hidden value in encrypted format in the final polynomial:

The Sum of the Polynomials after recovering the secret at each party is ::

(37)X^2 + (19)X^1 + (12)X^0

The secret value 12 computed by each party without knowing part of secret share of other party.

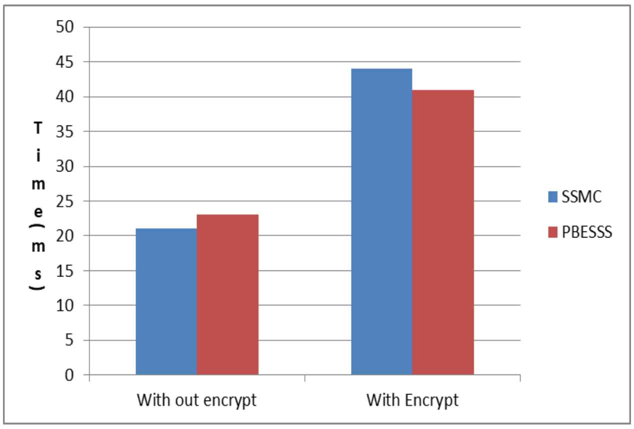

Figure:-1 Time analysis between schemes in milliseconds.

In our proposed scheme time taken in SSMC with encryption is more when compared to our proposed scheme PBESSS. Graph is plotted by taking number of parties and time taken in milli seconds.

VII. CONCLUSION

In this paper SMC based on Shamir is studied and a new scheme Polynomial Based Encryption Secret Sharing Scheme (PBESSS) is proposed for enhancing data security and privacy in multi-party computation mechanism which is extended to multi-cloud federation , results are given and analysed. The entire scheme PBESSS is applied to cloud entities participating for group computation mechanism in federation by sharing secret and at the same time it is encrypted as it cannot be modified at storage and in transit.

REFERENCES

1. Talalal Mousa Ibrahim Abdullah Althamary Alkharobi, Stable Multi-cloud File Sharing Using the Secret Exchange of Shamir Scheme, network transfers and ISSN: 2054 - Correspondence, Volume 4, Issue 6 7420 7420
2. Appistry Inc., “Cloud Platforms vs. Cloud Infrastructure”, 2009 White Paper .
3. Rajkumar Ranjan and Rajiv Buyya and Rodrigo N. Calheiros,"Service-Federation of Concentrated Inter Cloud. Cloud Environment Computing Application Services Scaling," Part I, LNCS 6081, Springer, ICA3PP,2010,Springer. 2010, pages 13-31. DIO: 01/10/978-3-642-13119-
4. D. Chaum, I, and C. Crepeau. Damgard. Damgard. Non- Multi Group protected protocols unconditionally (extended Abstract)" Abstract). In Proc. In Proc. STOC 20th, pages11-19, 1988 1988
5. Tartu Academy, Tartu Institute, Dan Bogdanov Computer science, foundations and properties Shamir's secret tool for science sharing
6. Seminar on Cryptography ,May 1st, 2007.
7. "The Discrete Logarithm, Kevin S. McCurley Issue," Symposium proceedings in Applied Math, Volume 42, 1990 George R Blakley.
8. Cryptographic safeguarding Keys. In AFIPS 1979 national hearings Computer Meeting, volume 48, pages 313– Computer Conference. 317, 1997.
9. Shamir Adi. How do I share a password. 22(11):612–613, ACM Correspondence, 1979. 1979.
10. Ivan Damgard. Secret sharing. Course notes, 2002. Tieng, Deneisha Gayle & Nocon, Ederlina. (2016). Some Attacks on Shamir's Secret Sharing Scheme by Inside Adversaries.
11. Mu Yang,Andrea et.al, *Differentially Private Data Sharing in a Cloud Federation with Blockchain*, IEEE Cloud Computing ,November/December 2018
12. http://www2.siit.tu.ac.th/prapun/tcs455 /ece561%2005%2001%20Polynomials%20over %20Galois%20Field.pdf.

AUTHORS PROFILE

Mrs. V. Keerthi pursued Master of Computer Science from Sri Venkateswara University, Tirupathi. She has pursued her Master of Philosophy in Computer Science from Dravidian University, Kuppam. She is currently pursuing Ph.D. in Dravidian University, Kuppam. Her main research work focuses on Cryptography and cloud computing. She is having 4 years of teaching experience. She has published 3 International Journals.
Mail id**: keerthiuha@gmail.com**

Prof. T. Anuradha pursued Master of Computer Applications from Sri Padmavathi Mahila Viswa Vidyalayam, Tirupati. She has pursued her Ph.D. from Sri Padmavathi Mahila Viswa Vidyalayam, Tirupati. She is working as the Professor in the Department of Computer Science. Presently she is the Vice Chancellor (i/c) of Dravidian University. Her Areas of Research Interests are Data Mining & data warehousing, Neural Networks, Cloud computing, Wireless Sensor Networks. She has the Publication record of 40 International Journals.