A Implementation of Secure and Strategic E-Voting System using the Algorithmic Security Visualization

Bimal Kumar, M. Siddappa

Abstract: - E-Voting is one of the advance techniques which is imposed for the Voters to a get advancement in casting their vote towards to their desired candidate. The E-Voting is implemented in various other countries with the various methodologies as per their need. This paper evaluates a Unique method for the process of e-voting with the proper authentication from the government servers and also it authenticates the e-Voting machine using the proper authentication process and allows the voter to cast their vote towards the desired candidate. The System uses the Specific Security Strategic Algorithm which is used for the providing of the efficient security to the both Voter and Voter Machine. The Chances of the Jail Breaking of the Communication channel of the system server and e-Voting Machine is reduced to minimal level that the no chances of data breach or the data leak can be entertained. Following of the proper architectural approach which makes the system more efficient which achieves the higher range of the accuracy and throughput value when compared with the other imposed E-Voting System. The strategic policies used in the system complies with all the security rules and terms that provides the evidences of a better architecture gives the process of the E-Voting system more secure and specific

Index Terms: - E-Voting System, Security, Integrity, Communication Channel Security.

I. INTRODUCTION

Secure and sensible choices and casting a voting are the essential components for an evenhanded nation. Choices license the majority to pick their agents express their tendencies for how they will be spoken to. Thusly, the uprightness moreover, precision of race process is essential to the uprightness of the greater part manages framework itself. Today, some new mechanical progressions are making. Thusly, web business security and sensible exchange including electronic casting a voting is transforming into an outstanding example. As such, analysts from Myanmar start to displace electronic casting a voting instead of regular paper casting a voting for saving human resource and time. Thusly, the execution of secure electronic casting a voting system is particularly fundamental in every nation.

The guideline target of e-Voting is to give voters a respectable condition so voters can cast their votes with least expense and attempts. There are such tremendous quantities of properties that have been proposed to make the e-Voting secure procedure.

Casting a voting is major in our forefront social requests. As per this, compact applications are being created and sent on cutting edge cells to impact the casting a voting to process significantly increasingly direct and convincing. These applications have raised our lifestyle whereby people can direct the whole world at their fingertips‟-casting a voting system have been familiar with update a couple of features of the representative strategy [1]. It is generally observed as a mode for propelling lion's share rules framework, setting up confidence in constituent organization, adding genuineness to choose outcomes what's more, upgrading the general adequacy of the representative method [2]. It is a reality that, with fitting use, on the web casting a voting system can discard a couple of cheats, pace up the preparing of results and make casting a voting increasingly appropriate for the open.

In any case, if not certainly considered and plot, web casting a voting may destroy the trust in the entire constituent procedure [2,3]. This investigation work inspects the layout of an online casting a voting system that can be used at school level to proceed with their yearly choice. This system will be an all-around7 paperless one since it will discard all the manual endeavors. Understudies can get to the application on their PDA, wherever and at whatever point they need and pick their understudy bodies gave they have web affiliation. Understudies will never again need to sit tight for stretch out timeframes to get the result since the structure will give ceaseless results It viably met its focuses moreover, goals and all of the necessities determined before were met. It will be helpful for the Clients who wish to cast a voting since the casting a voting technique will be made straightforward by using this application. Regardless, in the wake of having attempted the structure, in future we will in general incorporate additional helpfulness of picture endorsement for the security confinement and uniqueness which will give very strong security to the private information about vote. Furthermore, an initiation clock can be familiar with set the start and conclusion time of the race. Near to, the Clients are instructed of the starting time through a message and can start casting a voting. Amidst, estimations are given and once the clock is done, the casting a voting procedure is blocked normally and the Clients can simply see the last results.

Revised Manuscript Received on November 22, 2019

Bimal Kumar, Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool, Andhra Pradesh, India, vmlkumar80@gmail.com

Dr.M.Siddappa Professor, Department of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India, siddappam@ssit.edu.in

Retrieval Number: D7167115419 /2019©BEIESP
DOI:10.35940/ijrte.D7167.118419

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. PROPOSED ARCHITECTURE

The proposed architecture constitutes the strategic implementation of the system which comprises of the proper communication channel which provides the exact method through which the e-Voting System becomes more efficient.

The architecture which comprises of the interaction of user and infrastructure public and private servers fully under control of Government for the efficient authentication of the user. The System should be kept in the private state that all the security protocols which is needed for the proceeding of the system as the e-Voting system will be prioritized in the system. The user has to self-authenticate himself using the system authentication methodology which comprises of the verification from the Public and Private server. The servers which uses the two level authentication protocol which makes the servers reliable at all the perspective with other servers.

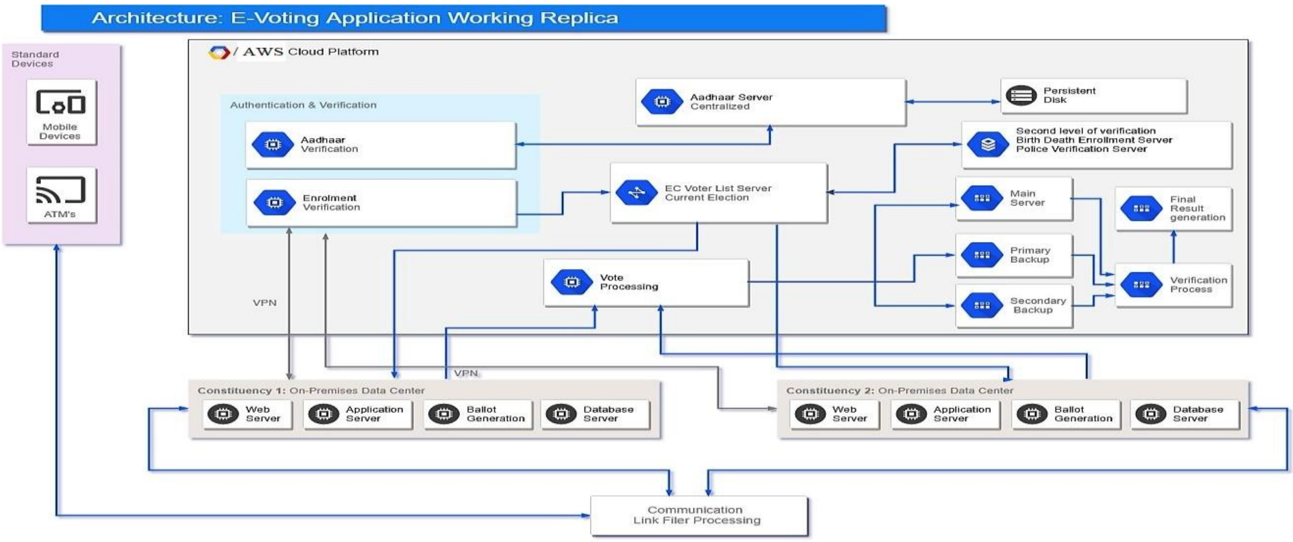

Architecture: E-Voting Application Working Replica
Standard Devices
Mobile Devices
ATM's
/ AWS Cloud Platform
Authentication & Verification
Aadhaar Verification
Enrolment Verification
Aadhaar Server Centralized
Persistent Disk
Second level of verification Birth Death Enrollment Server Police Verification Server
EC Voter List Server Current Election
Main Server
Final Result generation
Primary Backup
Vote Processing
Verification Process
Secondary Backup
VPN
VPN
Constituency 1: On-Premises Data Center
Web Server
Application Server
Ballot Generation
Database Server
Constituency 2: On-Premises Data Center
Web Server
Application Server
Ballot Generation
Database Server
Communication Link Filer Processing

Fig 1: - Overall Architecture for the Proposed e-Voting System EVC V1.8

A. Client Side Architecture

The client-side architecture which discuss with the overall performance of the system with respect to its working performance. The system will contribute with the client side as the user of the system plays more important role in the architecture. The E-Voter has to prove himself as the authenticated voter as the all the credentials which is being given by the user will be accredited with the government server with respect to the data which is present in the government repository. The Client side parts which associates with the entire segment side of the Client connection will connect to the dedicated constituency server the voter belongs to. The Client is the individual who takes on the framework for the e-throwing of their particular votes. The Client-side server which acts the Client end for the individual Client to make their choice. In the Client end, the gadget which is taken for the making of the choice is mulled over, In this area. The sectored e-casting a ballot gadget is confirmed by the different validation process for the fruitful throwing of the information verification convention.

The Client side part is associated with a transitory database and concentrated server called constituency server. The brief database which holds the information which comprise of the information consistency which gets the client information from the different sort of the casting a ballot gadgets and is put away in the transitory database where the impermanent database is associated with the steering convention which has set up its controlled association with the brought together database.

The incorporated server which has its inner and dynamic association with the cloud server through makes a productive method to make the information which is being created from the Client side gadget. An exemplary e-casting a ballot structure must play out most by far of these endeavors while consenting to a course of action of benchmarks developed by managerial bodies, and ought to moreover, have the option to deal successfully with strong requirements related with security, exactness, decency, speed, insurance, auditability, accessibility, cost-sufficiency, flexibility and natural supportability.

Electronic casting a ballot advancement can fuse punched cards, optical yield casting a ballot systems and explicit casting a ballot corners (tallying autonomous direct-recording electronic casting a ballot structure, or DRE). It can in like manner incorporate transmission of tickets and votes by methods for telephones, private PC frameworks, or the Internet.

B. The Server-Side Architecture

The server-side part includes the information which speaks to the information which is being refreshed from the Client end. The information which is being shared from the Client end is contemplated and is abutted to the involving server to find a way to store it in the variable space. At the point when the Client-side part is actuated and the Client begins the confirmation technique from the casting a ballot machine. The solicitation is sent to the server side for the general verification and information organization.

The server attempts to verify the Client data that is given by the Client by the all-out data that is accessible in the Aadhar seeding server. The information is gotten from the Aadhar seeding server for the best possible validation with the information that is given by the Client. At the point when every one of the directions that is being given by the Client and information sharing server matches, at that point the confirmation is fruitful.

The Secondary verification is taken into the thought with the unique finger impression confirmation that is furnished by the Finger Print Server / Aadhaar sever with its relating database. When the unique mark information confirmation solicitation made from the Client side for the Making of the choice. The unique mark solicitation is gotten from the voter gadget and is sent to the unique mark verification database for the getting to and effective validation of the information. On the post verification the voter is permitted to make his choice.

The third validation server is the area getting to server. Every single voter ought to be confirmed with the labeled server called the constituency server where the area of the voter is available. The definite area of the voter is shared from the casting a ballot gadget of the specific client. Through this area shared from the voter's information that is shared is coordinated with the current information that is available in the location sharing database. Ballot generation happens at constituency server as the list of candidates in the ballot made available to the constituency server so that the unique ballot generation process can be achieved successfully. Later On the effective coordinating the voter is permitted to make his choice. But before all this in the background voter verification happens at birth and death log server, police records will be verified to check the eligibility of the voter.

The last confirmation is done from the server side as for the different incidental information that is given by the client. That information which is being taken out is given for the cross confirmation with the information sharing server and through that all the checking information of the client is contemplated and that is cross confirmed with existing information in the information sharing server. At the point when all the four getting to servers are gives the correct confirmation which prompts the making of e-choice by the spoke to voter of the supporters

III. IMPLEMENTATION OF THE PROPOSED ALGORITHM FOR THE SECURITY

The Proposed structure uses the Data Security computation which is the homomorphic estimation which uses the single key for the encryption of data and moreover unscrambling of the data. The Grid Computing structure which is being used in the proposed system is restricted with the proposed figuring through which the whole system is kept in the separated security structure where the administrator or the Client of the structure should deal the security system using the Homomorphic Token key which is being delivered at the period of the constraining of the security data. In the recently referenced designing the Client has input his capabilities that is given when the mining assignments is made. The User on contributing the affirmations is checked with the capabilities database. Post the affirmation method the Client gets the powerful access to the key check module which where the key that is being inputted by the Client is checked by the key that is being made from the key transport center. In case the both keys are facilitated the Client gets the passageway rights to go into the mining plan and play out the mining exercises. If the Client doesn't get the passage approval, by then the Client isn't allowed into the system for the performing of the mining assignments.

```
Algorithm for Encryption of Data

Input: Ballot Vote Data (Total Data)
Output: Vote Encryption
Start
For each input in A do:
        If (Ballot Data= Voted Casted Data G
        {(Total, Attribute})


         Initialize the Data Encryption;
         Ma=AMa+ {(AMa, Signature)}
         Else if (input! has attribute in G)
         Ma=AMa
 Return Ma
 End
```

Algorithm 1: Algorithm for Encryption of Data

The Above referenced count is used for the powerful encryption of data which is being secured in the database, the key is made reliant on the data which is being secured in the database. The Key Distribution center holds all the keys which is being made from the encryption approach.

```
Key Generation Algorithm

Input: Ballot Credentials
Output: Access Rights Upon Successful
Verification of Key for Admin
Start
For each ballot input Key A
        If Input A →Ma (KCC)
        Check the B=Ma (KCC)
        If Yes
                Allow the Admin to Access the
Data in the Cloud
        Else
        Revoke the String Access of Admin
        Then
        Repeat the Key A,
Return Access Rights to Admin
End
```

Algorithm 2: Key Generation Algorithm

Once the Ballot Machine is completely encrypted the Client end can be staking final work of making the system more compliant

```
Algorithm for Decryption of Data
_______________________________________________
Input: Ballot Vote Data (Total Data)
Output: Vote Decryption
Start
For each input in A do:
        If (Ballot Data= Voted Casted Data G
        {(Total, Attribute})
        Initialize the Data Decryption;
        Ma=AMa+ {(AMa, Signature)}
        Ma=AMa+ {AMa+, Signature, Key,
        KCC Data)
        Else if (Decrypt in G)
        Ma=AMa+
Return Ma
End
```

Algorithm 2: Algorithm for Decryption of Data

with the user to make the client the access right to cast their vote and make the vote directly reach the respective repositories to make the vote counting more efficient Threshold returning Rate (TRR), whereas the TER corresponds with the Typical Error rates with the number of the input servers for the ballot generation, The SER corresponds with the Systematic Error which arises when the Ballot is generated and served for the casting,

The TRR Corresponds with the Returning radius of the ballot with respect to the TER and SER, also it comprises of the total threshold that is being generated by the E-voting system with respect to the Encryption and Decryption of the Data that is being provided from the Ballot Machine with respect to the value.

A. Implementation of Hardware Topology and Security Policies using simulation tool

The Systematic Generation of the Hardware Topology is need for the high-end data transfer from the Client end to the Server End. Some other sorts of the Security Policies are inducted to check the systematic presence of the security in the whole system using simulation tool packet tracer.

a. Inbound-User Access Control list

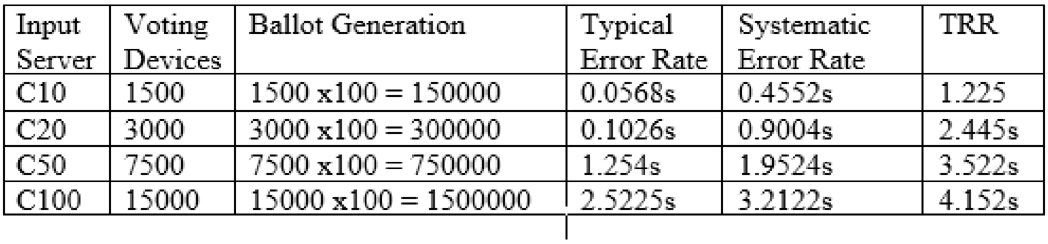
The total list of the user who we are the beneficent of the system is to be generated as the final list. And those who are having their user access grant permission in the list can only access the system

b. IPSec Protocol

The IPSec Protocol is used to the build the security to the Internet Protocol through which the communication channel is going to be Created.

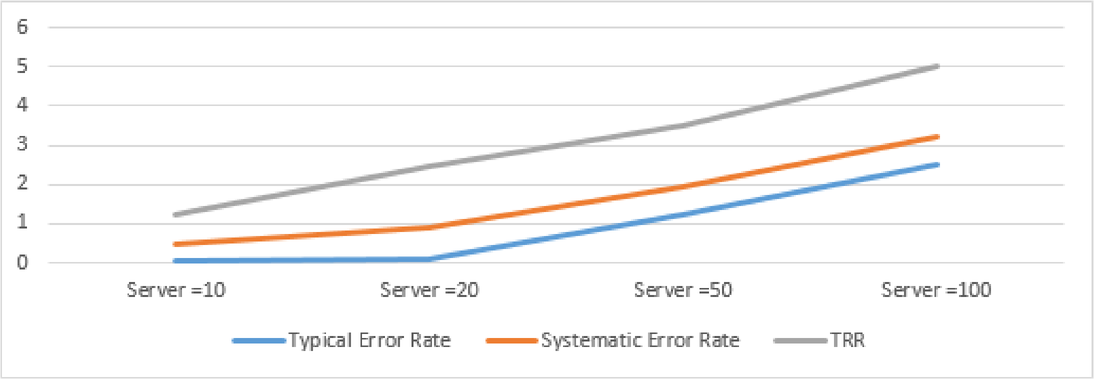
c. Port Binding

A port binding is the configuration data that determines where and how a message will be sent or received.



Input Server	Voting Devices	Ballot Generation	Typical Error Rate	Systematic Error Rate	TRR
C10	1500	1500 x100 = 150000	0.0568s	0.4552s	1.225
C20	3000	3000 x100 = 300000	0.1026s	0.9004s	2.445s
C50	7500	7500 x100 = 750000	1.254s	1.9524s	3.522s
C100	15000	15000 x100 = 1500000	2.5225s	3.2122s	4.152s

Table 1: Total number of Servers and its Capacitated Ballot Generation with TER, SER and TRR



Graph 1: Server Rate with Respect to TER, SER and TRR

d. HTTPS Communication

The Secured HTTPS communication is used to provide the security from the end level user to the server admin to avoid the attacks on the communication channel to disintegrate the data.

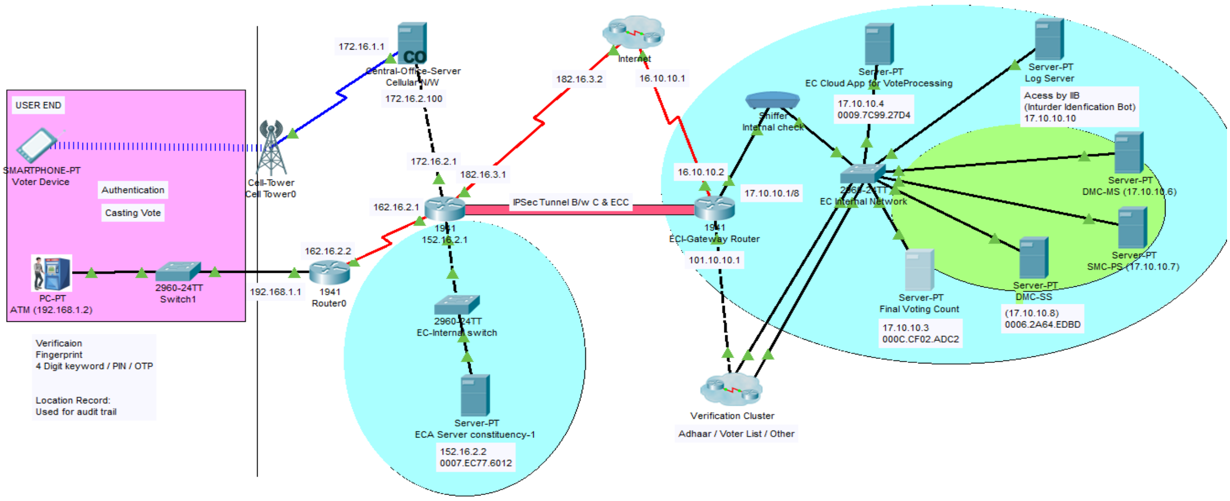


Figure 2: Simulated setup for the architecture shown in figure 1 to check the implementation of hardware topology and security policies

e. Log Server Configured with Intruder Identification Bot

An Automated Bot is deployed to check the possibility of intrusion and any direct or indirect Intruders with the socket address to find them.

f. Communication Methodology

The Client Concerned Application is being given with the access grant only to access the front server namely constituency server which is intended to assist the client. The client cannot have the direct access to the Vote Server.

g. Sniffer Hardware

The sniffer hardware is also used to find the attack possibilities and hacking possibilities in the both Hardware and Software End.

h. Cloud Implementation

All the Server are directly connected to the cloud for the data transmission and storing. The Hybrid cloud is used for the server implementation which constitutes many advantages.

i. Secret Sharing and Triple Stake Holder Concept

To access the server which is being possessed with the data which is being sent from the voting server needs the three generated keys which is being generated when the data is encrypted. The Key Distribution Center is maintained for the Key Distribution among the respective need.

The Security key will be generated and distributed among three stake holders

1. Election Commission
2. Ruling Party Representative
3. Opposition Party Representative

All the Generated three keys will be in the Encrypted format and those data accessing grant permission will be given only when the three stake holders represent their individual key with respective to each other in the Server Authentication.

j. Double encryption and triple backup (DETB)

For better security and reliability and audit process as per the architecture double encryption has been done with triple backup. In will increase the reliability in the system and make the audit process easy.

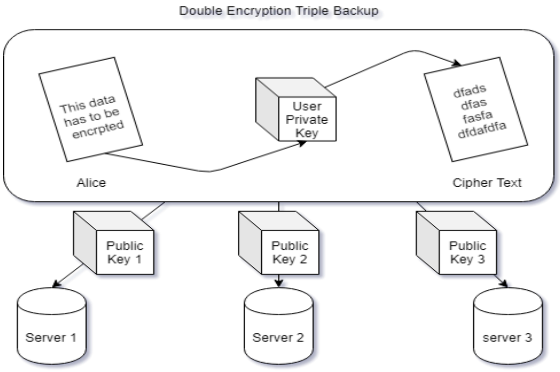


Fig 3: Double Encryption Triple Backup Architecture

IV. CONCLUSION

This paper proposes a novel method for the encryption and decryption of the data which is being sent from the e-voting system. E-Voting is one of the development system which is forced for the Voters to a get progression in making their choice towards to their ideal applicant. The E-Voting is actualized in different nations with the different strategies according to their need. This paper assesses a Unique technique for the procedure of e-casting a ballot with the correct validation from the administration servers and furthermore it verifies the e-Voting machine utilizing the best possible confirmation process and enables the voter to make their choice towards the ideal up-and-comer. The System utilizes the Specific Security Strategic Algorithm which is utilized for the giving of the proficient security to the both Voter and Voter Machine. The Chances of the Jail Breaking of the Communication channel of the framework server and e-Voting Machine is decreased to negligible level that the no odds of information rupture or the information hole can be engaged. Following of the best possible building approach which makes the framework increasingly proficient which accomplishes the higher scope of the precision and throughput esteem when contrasted and the other forced E-Voting System. The vital approaches utilized in the framework consents to all the security decides and terms that gives the confirmations of a superior design gives the procedure of the E-Voting framework increasingly secure and explicit.

REFERENCES

1. C. Castillo, G. Rouskas, and K. Harfoush, “On the Design of Online Scheduling Algorithms for Advance Reservations and QoSin Grids,” Proc. IEEE Int’l Conf. Parallel and Distributed ProcessingSymp. (PDP),pp. 1-10, Mar. 2007.
2. N. Doulamis, A. Doulamis, A. Panagakis, K.Dolkas, T. Varvarigou,and E. Varvarigos, “A Combined Fuzzy -Neural Network Modelfor NonLinear Prediction of 3D Rendering Workload in GridComputing,”IEEE Trans. Systems, Man, and Cybernetics (SMC)-Part-B,vol. 34, no. 2, pp. 1235- 1247, Apr. 2004.
3. E. Arkin and E. Silverberg, “Scheduling Tasks with Fixed Startand End Times,”Discrete Applied Math.,vol. 18, no. 1, pp. 1-8, 1987.
4. R.W. Lucky, “Cloud Computing,”IEEE Spectrum, vol. 46, no. 5,p. 27, May 2009.
5. K. Singh, E._Ipek, S.A. McKee, B.R. de Supinski, M. Schulz, and R.Caruana, “Predicting Parallel Application Performance via Machine Learning Approaches,” Concurrency and Computation:Practice & Experience,vol. 19, no. 17, pp. 2219-2235, Dec. 2007.
6. M. Maheswaran, K. Krauter, and R. Buyya, “A Taxonomy and Survey of Grid Resource Management Systems for Distributed Computing,”Software: Practice and Experience, vol. 32, no. 2,pp. 135-164, Feb. 2002.
7. R.J. Al-Ali et al., “Analysis and Provision of QoS for Distributed Grid Applications,”J. Grid Computing,vol. 2, pp. 163-182, 2004.
8. M.S. Fineberg and O. Serlin, “Multiprogramming for Hybrid Computation,”Proc. IFIPS Fall Joint Computer Conf.,1967.
9. A. Stankovic et al., “Implications of Classical Scheduling Results for Real Time Systems,” Computer,vol. 28, no. 6, pp. 16-25, June 1995.
10. P. Kokkinos and E. Varvarigos, “A Framework for Providing Hard Delay Guarantees and User Fairness in Grid Computing,” Future Generation Computer Systems,vol. 25, no. 6, pp. 674-686, 2009.
11. D. Jackson, Q. Snell, and M. Clement, “Core Algorithms of the Maui Scheduler,”Proc. Seventh Int’l Workshop Job Scheduling Strategies for Parallel Processing (JSSPP),pp. 87-102, 2001.
12. B. Bode et al., “The Portable Batch Scheduler and the Maui Scheduler on Linux Clusters,”Proc. Usenix Conf.,2000.
13. “Platform Computing Corporation,” http://www.platform.com, 2013.
14. H. Casanova, A. Legrand, D. Zagorodnov, and F. Berman,“Heuristics for Scheduling Parameter Sweep Applications in Grid Environments,”Proc. Ninth Heterogeneous Computing Workshop, pp. 349- 363, 2000.
15. R. Buyya, M. Murshed, D. Abramson, and S. Venugopal,“Scheduling Parameter Sweep Applications on Global Grids: A Deadline and Budget Constrained Cost-Time Optimisation Algorithm,”Software: Practice and Experience,vol. 35, pp. 491-512, 2005.
16. N. Doulamis, A. Doulamis, E. Varvarigos, and T. Varvarigou, “Fair Scheduling Algorithms in Grids,”IEEE Trans. Parallel and Distributed Systems,vol. 18, no. 11, pp. 1630-1648, Nov. 2007.
17. K. Rzadca, D. Trystram, and A. Wierzbicki, “Fair Game-Theoretic Resource Management in Dedicated Grids,”Proc. IEEE Seventh Int’l Symp. Cluster Computing and the Grid (CCGrid), pp. 343- 350,2007.
18. V. Martino and M. Mililotti, “Scheduling in a Grid Computing Environment Using Genetic Algorithm,”Proc. 16th Int’l Parallel and Distributed Processing Symp.,p. 297, Apr. 2002.
19. S. Kim and J. Weissman, “A Genetic Algorithm Based Approach for Scheduling Decomposable Data Grid Applications,”Proc. IEEE Int’l Conf. Parallel Processing (ICPP),pp. 406-413, Aug. 2004.
20. .20. G. Ye, R. Rao, and M. Li, “A Multiobjective Resources Scheduling Approach Based on Genetic Algorithms in Grid Environment,” Proc. Fifth Int’l Conf. Grid and Cooperative Computing Workshops (GCCW ’06),pp. 504-509, Oct. 2006.
21. W. Smith, I. Foster, and V. Taylor, “Scheduling with Advanced Reservations,” Proc. 14th Int’l Parallel and Distributed Symp. (IPDPS),pp. 127-132, 2000.
22. E. Varvarigos, N. Doulamis, A. Doulamis, and T. Varvarigou, “Timed/Advance Reservation Schemes and Scheduling Algorithms for QoS Resource Management in Grids,”Engineering the Grid,pp. 355-378, Am. Scientific Publishers, 2006.
23. I. Foster, C. Kesselman, C. Lee, R. Lindell, K. Nahrstedt, and A. Roy, “A Distributed Resource Management Architecture that Supports Advance Reservation and Co-Allocation,”Proc. Seventh Int’l Workshop Quality of Service (IWQOS), pp. 27-36, 1999.

AUTHOR PROFILE

Bimal Kumar is currently a Research Scholar in Department of Computer Science, Rayalaseema University, Kurnool. He is pursuing the Research in the area of Network and Data Semantics on the E-voting System.

Dr.Siddappa.M is currently Professor in Department of Computer Science and Engineering, Sri Siddartha Institute of Technology, Tumkur. He has 28 years of Teaching Experience and 8 years of Research Experience. His current area of Interest are Data Structure, Artificial Intelligence and Computer Networks