ISSN Applicaiton No. 21727

Global Journal of Programming Languages

Volume No. 8

Issue No. 3

September - December 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN Applicaiton No. 21727

Global Journal of Programming Languages

Aims and Scope

Global Journal of Programming Languages is a peer-reviewed Print + Online journal of Enriched Publications to disseminate the ideas and research findings related to all sub-areas of programming languages. It also intends to promote interdisciplinary researches and studies in computer science maintaining the standard of scientific excellence. This journal provides the platform to the scholars, researchers, and PHD Guides and Students from India and abroad to adduce and discuss current issues in the field of programming and Computer Sciences.

ISSN Applicaiton No. 21727

Global Journal of Programming Languages

ISSN Applicaiton No. 21727

Global Journal of Programming Languages

(Volume No. 8, Issue No. 3, September - December 2023)

Contents

Cloud Infrastructure using Software Agent – A Review

Amit Kapoor[1]

[1]Assistant Professor, Maharaja Agrasen Institute of Management and Technology,
Jagadhri, Haryana, India

ABSTRACT

Cloud computing provides virtualized resources and scalable infrastructure in the form of services over the Internet. It is a model for enabling on-demand network access to a shared pool of computing resources. Cloud infrastructure is implemented on virtual machines which are remotely located. Any user who wants to access his data or any application has to send request to cloud service provider who intern replies with an address or a pointer to the services. Agent- based Cloud computing must be set for providing agent-based solutions founded on the design and development of software agents for improving Cloud resources and service management , discovery and service composition. Autonomous agents can make Clouds smarter in the interaction with users and more efficient in allocating processing and storage to applications. In large-scale data centers, agents can search, filter, query and update the massive volumes of data that are stored. We study the architecture of agent based clouds using multi agent system.

Keywords: VMs, Cloud Computing, Agents, Saas, Paas, Iaas

1. INTRODUCTION

Cloud computing provides dynamically scalable infrastructure or virtualized resources in the form of services over the Internet. It is a model for enabling scalable, on demand network access to a shared pool of configurable computing resources that can be provisioned ubiquitously and released with minimal management effort and cloud service provider interaction. Cloud computing paradigm uses virtualization approach to provide resources to the users on which they have full administrative control. Cloud infrastructure is implemented on VM's which are remotely located. Any user who wants to access his data or any application has to send request to cloud service provider who intern replies with an address or a pointer to the services. Existing cloud infrastructures use virtualization techniques with hypervisors to transparently allocate resources of physical hosts for a service provider's virtual machines (VMs). A key benefit of virtualization is that it allows running multiple operating systems on a single physical system where underlying hardware resources are shared.

2. LITERATURE REVIEW

According to Rajkumar Buvaya (2009), Agent-based Cloud computing is concerned with the design and development of software agents for bolstering Cloud service discovery, service negotiation and service composition. The significance of this work is introducing an agent-based paradigm for constructing software tools and testbeds for Cloud resource management. Novel contributions of this work include:1) developing Cloudle: an agent-based search engine for Cloud service discovery, 2) showing that agent-based negotiation mechanisms can be effectively adopted for bolstering Cloud service negotiation and Cloud commerce, and 3) showing that agent-based cooperative problem-solving techniques can be effectively adopted for automating Cloud service composition. Cloudle consists of a service discovery agent that consults Cloud ontology for determining the similarities between providers' service specifications and consumers' service requirements. To support Cloud commerce, this work devised a complex Cloud negotiation mechanism that supports parallel negotiation activities in interrelated markets.Empirical results show that using such mechanism, agents achieved high utilities and high success rates in negotiating for Cloud resources. To automate Cloud service composition, agents adopt the contract net protocol (CNP) and use acquaintance networks (AN). Empirical results show that using CNP and AN, agents can successfully compose Cloud services by autonomously selecting services.

According to Rafel (2010), Cloud computing is gaining acceptance in many IT organizations, as an elastic, flexible and variable-cost way to deploy their service platforms using outsourced resources. Unlike traditional utilities where a single provider scheme is a common practice, the ubiquitous access to cloud resources easily enables the simultaneous use of different clouds. This paper explores the scenario to deploy a computing cluster on top of a multi-cloud infrastructure, for solving loosely-coupled Many-Task Computing (MTC) applications. In this way, the cluster nodes can be provisioned with resources from different clouds to improve the cost-effectiveness of the deployment, or to implement high-availability strategies.

According to Aarti Singh (2012), Cloud computing focuses on delivery of reliable, secure, fault tolerant, sustainable, and scalable infrastructures for hosting internet-based application services. These applications have different composition, configuration, and deployment requirements. Cloud service providers are willing to provide large scaled computing infrastructure at a cheap prices.

Quantifying the performance of scheduling and allocation policy on a Cloud infrastructure (hardware, software, services) for different application and service models under varying load, energy performance (power consumption, heat dissipation), and system size is an extremely challenging problem to tackle. This problem can be tackle with the help of mobile agents. Mobile agent being a process that can transport its state from one environment to another, with its data intact, and is capable of performing appropriately in the new environment. This work proposes an agent based framework for providing scalability in cloud computing environments supported with algorithms for searching another cloud when the approachable cloud becomes overloaded and for searching closest datacenters with least response time of virtual machine (VM).

According to Divya Jyothi(2012),In this paper secure dealer agent mechanism is implemented to provide market oriented approach by using cloud computing environment. Cloud by leveraging technologies, provides thought on market based resource management strategies that encompasses customer driven service management. The resources lie in a large stockpile in agent, from where it would be accessible to everyone. The Technology provided by the cloud for consider implement market oriented for providing services to the consumers. The services provided by the cloud computing to the providers pay for the services. Paper deals with ecommerce dealer agent mechanism transaction that enables business minded approach for the customers which is carried out from cloud computing. The main aim of the paper is to implement the mechanism such that the dealer is the actual ecommerce sites who will add its own product to the agent database. Agent is the one who will maintain all ecommerce sites product database and payment database. Agent searches the product in which ecommerce site the product is available. To start with web services enables the agent to service the product JAX-WS (web service) is used. Trading system is brought in a sense enabling trading. Direct payment is the default feature for buying product which then security concern is solved by PayPal sandbox implementation for secure transaction. The load impact performance of individual website is measured by using Load impact tool.

3. CLOUD COMPUTING ARCHITECTURE

Architecture of cloud computing mainly comprises of four layers: Hardware, Infrastructure, Platform and Application. These four layers facilitate three different types of cloud services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These layers are described in detail as follows

Figure1: Cloud Computing Environment

• **Software as a Service (SaaS):** This service allows the consumer to use desired softwares from the cloud infrastructure. SaaS is a model of software deployment whereby a provider licenses an application to customers as a service for on demand usage. The software applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumers has no need to manage or control the cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. SaaS therefore alleviates the customer's burden of software maintenance, reduces the expense and improves the operational efficiency of software purchases by on-demand pricing. One example of SaaS is the Salesforce.com CRM (Customer Relationship Management) application.

• **Platform as a Service (PaaS):** This layer is responsible for providing resources such as Operating System and software development frameworks. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and hosting environment configurations. Major purpose of PaaS is the delivery of a computing platform and solution stack as a service. It facilitates the deployment of applications without the cost and complexity of buying and managing the underlying software layers. It provides the facilities required to support the complete lifecycle of building and delivering web applications and services. An example of this would be GoogleApps and Microsoft Azure. This layer lies above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of development environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development lifecycle management, from planning to designing and building applications to their deployment, testing and maintenance.

• **Infrastructure as a Service (IaaS):** This layer provides the consumers with processing facility in the form of virtual machines (VMs), storage blocks, networking and other fundamental computing resources so that the consumer may deploy and run arbitrary softwares, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). IaaS completely changes the way of developers deploy applications. Instead of spending large funds on their own data centers, hosting companies or co-location services and then hiring operations staff to get it going, they can just go to Amazon Web Services EC2(Elastic Compute Cloud)4or one of the other IaaS providers, get a virtual server running in minutes and pay only for the resources they use. With cloud brokers like Rightscale, enStratus, etc., they could easily grow big without worrying about things like scaling and additional security. In short, IaaS and other associated services have enabled startups and other businesses focus on their core competencies without worrying much about the installation and management of infrastructure. IaaS is the delivery of computer infrastructure (typically a platform virtualization environment (Xen) as a service. Rather than purchasing servers, software, space for data center or network equipments, clients instead buy those resources as a fully outsourced service.

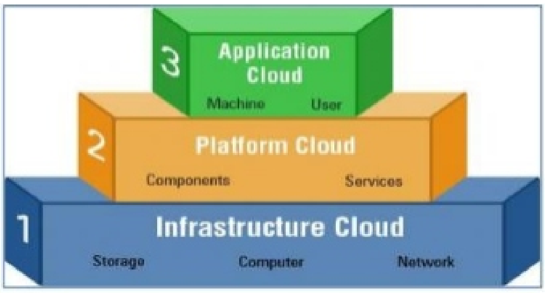


Figure2: Cloud Service Model

4. CLOUD DEPLOYMENT MODELS

About five years ago, when the first Cloud infrastructure has been deployed by Amazon, the online bookseller company that took the decision to start a new business selling computing resources to companies and private users, the only deployment model was the Public Cloud one. It is a pay-per-use IaaS Cloud infrastructure that is owned by an organization selling Cloud services to the general public or to enterprises. Thus, it is public because it can be rent by anyone for developing and/or running any kind of applications. To use Amazon services, users must provide a credit card account and can spend from few cents to thousands or millions of dollars depending on the number of used resources and the usage time. After this early Cloud version, other deployment models different from Public Clouds have been designed and implemented

- **Public:** available publicly - any organisation may subscribe

- **Private:** The Cloud infrastructure is owned or leased by a single organization and is operated only for that organization. No public access to it is permitted. This model can be used in case of strict data privacy and/or security requirements.

- **Partner or Community:** The Cloud infrastructure is shared by a limited number of organizations and supports a specific community that has shared concerns (e.g., goals, security requirements, policy, and compliance issues).

4.1 Cloud Computing Benefits

The benefits of deploying applications using cloud computing include reducing run time and response time, minimizing the risk of deploying physical infrastructure, lowering the cost of entry, and increasing the pace of innovation.

1. Reduce run time and response time
2. Minimize infrastructure risk
3. Lower cost of entry
4. Increased pace of innovation
5. Agents in Cloud Computing

An agent is a computational entity that acts on behalf of another entity (or entities) to perform a task or achieve a given goal. Agent systems are self-contained software programs embodying domain knowledge and having ability to behave with a specific degree of independence to carry out actions needed to achieve specified goals. They are designed to operate in a dynamically changing environment. Agents typically include a set of features.

• **Autonomy:** the capacity to act autonomously to some degree on behalf of users or other programs also by modifying the way in which they achieve their objectives.

• **Pro-activity:** the capacity to pursue their own individual set goals, including by making decisions as result of internal decisions.

• **Re-activity:** the capacity to react to external events and stimuli and consequently adapt their behavior and make decisions to carry out their tasks.

• **Communication and Cooperation:** the capacity to interact and communicate with other agents (in multiple agent systems), to exchange information, receive instructions and give responses and cooperate to fulfill their own goals.

• **Negotiation:** the capability to carry out organized conversations to achieve a degree of cooperation with other agents.

• **Learning:** the ability to improve performance and decision making over time when interacting with the external environment.

Although a single agent can act and run to perform a given task, the agent paradigm was conceived as a distributed computing model where a set of agents interact one another by exchanging information and cooperating to perform complex tasks where interaction, intelligence, adaptation and dynamicity are key issues to be handled.

1. Cloud Environment using Software agents

Cloud environment is considered to have three components clients, cloud service providers and Software agent. Now each component is explained below:

1. Client is the one who initiate request i.e. fulfilled by cloud service provider server. So that client never knows what is happening behind cloud environment.

2. Cloud Service Provider is a collection of System's (Servers) connected to each other that are running all time for full filling the client requests.

3. Software agents working on our and operating systems behalf, to provide intelligent data access services, monitoring services, processor-to-application assignment strategies, and energy-efficient use of Cloud computing infrastructures.

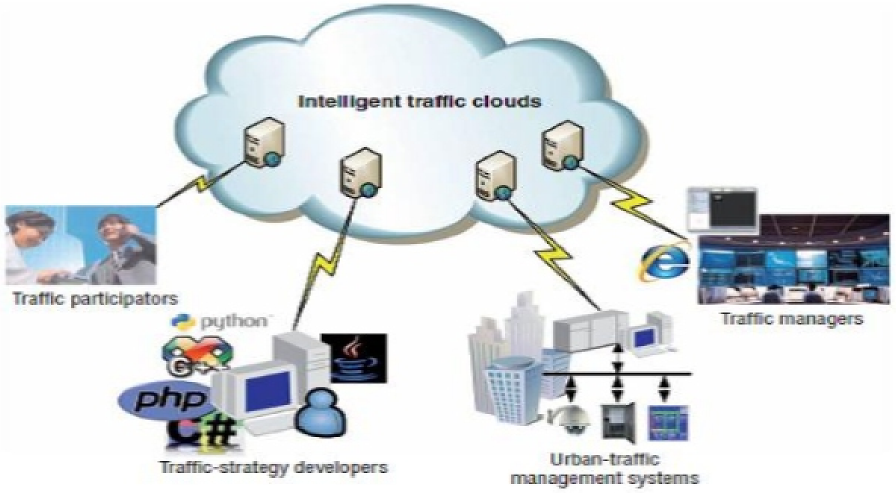

Intelligent traffic clouds
Traffic participators
python
php
C#
Traffic-strategy developers
Urban-traffic management systems
Traffic managers

Figure3: Cloud Service Model using Agents

6. Clouds Using Agents

Cloud computing is a novel technology that has been designed and implemented in the past few years, mainly due to industry that was looking to a large-scale scalable computing infrastructure for implementing and selling service-oriented commercial solutions. Whereas much of the current effort on Cloud computing was devoted to the production of Cloud infrastructures and technologies for supporting virtualization and data centers, little attention has been devoted to introduce innovative methods for users and developers to discover, request, assemble and use Cloud computing resources.

A new discipline, called agent-based Cloud computing must be set for providing agent-based solutions founded on the design and development of software agents for improving Cloud resources and service management and discovery, SLA negotiation, and service composition. Autonomous agents can make Clouds smarter in the interaction with users and more efficient in allocating processing and storage to applications.

In large-scale data centers, agents can search, filter, query and update the massive volumes of data that are stored. We can envision a scenario where Cloud agents working on our and operating systems behalf, to provide intelligent data access services, monitoring services, processor-to-application assignment strategies, and energy-efficient use of Cloud computing infrastructures.Research activities must be carried out to implement effective agent-based solutions for Cloud computing. This work should be done towards the three different *-as-a-Service delivery classes.

- In IaaS infrastructures, agents can be used to help the intelligent provisioning of basic resources to user applications,
- In Paas infrastructures, agent can play a role in the efficient deployment and execution of programming environments that developers use for application implementation.
- Finally, in SaaS Cloud infrastructures, agents can be programmed to optimize the use of applications provided as services and the management of the underlying hardware/software infrastructure taking care of its efficient utilization and, at the same time, for maintaining the declared QoS.

In Clouds, there also is the need to design and implement techniques and methodologies that adapt to the dynamic behaviors of Cloud computing environments. Autonomic techniques may help providers and users to reach this goal. Multi-agent systems that are able to handle with changing configurations, heterogeneity, and volatility, can provide a promising approach for addressing this requirement. Last but not least, security and trust are two very critical issues in Cloud computing as data and software are stored, accessed and run on machines that are not owned or directly managed by owners of data and software. Agent-based models and algorithms for trust and security in Cloud infrastructures could be very useful.

In summary, if agent-based solutions will be introduced in the software infrastructure of Clouds we will have:

- Intelligent and flexible Cloud services,
- Autonomous and pro-active services,
- Autonomic Clouds.

7. CONCLUSION

This paper discusses the agent based cloud computing using Agents. The main goal is to continuously supervising the system's in a cloud infrastructure so that if any of the systems fails to fulfill the request so that Software agent will redirect that request to some other system in a cloud so that client gets its requested information. The agent is active all the time so that it can perform task intelligently.

8. REFERENCES

[1] Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend". Future Networks, 2010. ICFN '10. Second International Conference. Jan. 2010.

[2] VMWare Staff, "Virtualization overview". White Paper: http://www.vmware.com/pdf/virtualization.pdf.

[3] White Paper: Introduction to CloudComputing.http://www.thinkgrid.com/docs/computing-whitepaper.pdf

[4] Boss, G., Malladi, P., Quan, D., Legregni, L. Hall, H.: "Cloud Computing". High Performance on Demand Solutions (HiPODS) by IBM, 2007.

[5] XenSource Inc, Xen, www.xensource.com.

[6] Domenico Talia "Cloud Computing and Software Agents: Towards cloud Intelligent Services", University of Calabria, Italy.

[7] K. P. Sycara, "Multiagent systems," AI Magazine, vol. 19, no. 2,pp.79-92, 1998.

[8] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal "Market Oriented Cloud Computing: Vision, Hype and reality for delivering IT Services as Computing Utilities" The University of Melbourne, Australia.

[9] Bo Peng "Implementation Issues of A Cloud Computing Platform" Department of Computer Science & Techonology , Peking University.

[10] Myougnjin Kim, Hyogun Yoon, Jee-In Kim, HyungSeok Kim " An Intelligent Multi-agent Model based on Cloud Computing for Resource Virtualization" International Conference on Information and Electronics Engineering IPCSIT vol.6 (2011) © (2011) IACSIT Press, Singapore.

[11] Aarti Singh, Manisha Malhotra "Analysis for Exploring Scope of Mobile Agents in Cloud Computing" International Journal of Advancements in Technology Vol. 3 No 3 (July 2012) ©IJOAT.

[12] Priyank Singh, Ranjita Singh,Mukul Singh "Security Agents : A Mobile Agent Trust Model for Cloud Computing"International Journal of Computer Applications (0975 – 8887) Volume 36– No.12, December 2011.

[13] Aarti Singh, Manisha Malhotra "Agent Based Framework of Scalability in Cloud Computing" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 3 No. 4 April 2012.

[14] Ms. Divya Jyothi , Prof. D. R. Ingle" Agent in E-commerce Application based on Cloud Environment " International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 6, August 2012

[15] Lopez-Rodriquez, M. Hernandez-Tejera, "Software Agents as Cloud Computing Services," Proc. 9th Int. Conference on Practical Applications of Agents and Multiagent Systems - PAAMS 2011, Springer, Salamanca, Spain, pp. 271-276, 2011.

[16] Cloud Computing Expert Group, "The Fuure of Cloud Computing," Report from European Commission, January 2010.

[17] M. Armbrust, et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, April 2010.

Interval Valued Intuitionistic Q- Fuzzy Graphs

R. Nagarajan*, K. Balamurugan**

* Associate Professor, Department of Mathematics, J J College of Engg& Tech, Trichirappalli-09

** Assistant Professor, M.A.M School of Engineering, Trichirappalli-105

ABSTRACT

In this paper, we introduce the notion of interval –valued intuitionistic Q-fuzzy graphs and describe various methods of their construction. We also present the concept of interval-valued intuitionistic Q-fuzzy regular graphs.

Keywords: Q-fuzzy set, Q-fuzzy graph, intuitionistic Q-fuzzy set, Interval-valued intuitionistic Q-fuzzy graph, Intuitionistic Q-fuzzy relation, Cartesian Product.

AMS Subject classification 2000: 05C99

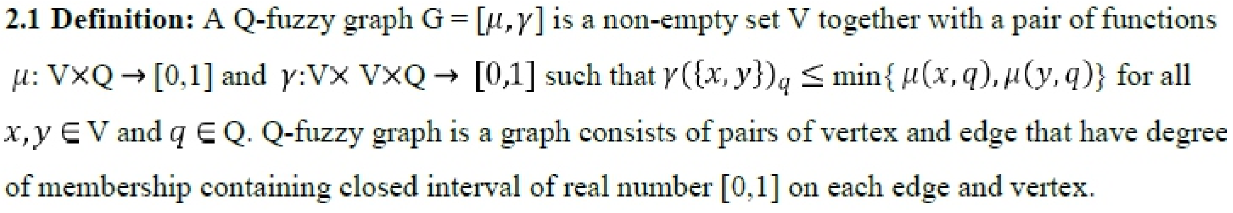
1. INTRODUCTION:

In 1736, Euler first introduced the notion of graph theory. In the history of mathematics, the solution given by Euler of the well known Konigsberg bridge problem is considered to be the first theorem of graph theory. This has now become a subject generally regarded as a branch of combinatories. The theory of graph is an extremely useful tool for solving combinatorial problems in different areas such as geometry, algebra, number theory, topology, operation Research, optimization and computer Science. In 1975 , Rosenfeld [8] introduced the concept of fuzzy graphs. The fuzzy relation between fuzzy sets were also considered by Rosenfeld and he developed the structure of fuzzy graphs, obtaining analogs of several graph theoretical concepts. Mordeson and Peng [4] introduced some operator on fuzzy graphs,. Shannon and Atanassov [7] introduced the concept of intuitionistic fuzzy relation and intuitionistic fuzzy graphs, and investigated some of their properties. Recently Akram and Dudek [1] have studied some properties of interval –valued fuzzy graphs. In 1975, Zadeh [10] introduced the notion of interval –valued fuzzy sets as an extension of fuzzy sets [11] in which the values of the membership degree are intervals of numbers instead of the numbers. The notion of interval –valued intuitionistic fuzy sets was introduced by Atanassov and Gargo [3] in 1989 as a generalization of both interval –valued fuzzy sets and intuitionistic fuzzy sets. Grrstenkorn and Manko [6] re- named the intuitionistic fuzzy sets as bi fuzzy sets in 1995. A.Solairaju and R.Nagarajan [9] have introduced and defined a new algebraic structure called Q-fuzzy subgroups.

In this paper, we introduce the notion of interval –valued intuitionistic Q-fuzzy graphs and describe various methods of their construction. We also present the concept of interval-valued Q- intuitionistic regular graphs.

2. PRELIMINARIES

We first recall some basic concept which are used to present the paper.



2.1 Definition: A Q-fuzzy graph G = $[\mu, \gamma]$ is a non-empty set V together with a pair of functions μ: V×Q → [0,1] and γ:V× V×Q → [0,1] such that $\gamma(\{x, y\})_q \leq \min\{\mu(x, q), \mu(y, q)\}$ for all $x, y \in$ V and $q \in$ Q. Q-fuzzy graph is a graph consists of pairs of vertex and edge that have degree of membership containing closed interval of real number [0,1] on each edge and vertex.

2.2 Definition: An interval number D is an interval $[a^-, a^+]$ with $0 \leq a^- \leq a^+ \leq \mathbf{1}$. The interval $[a, a]$ is identified with the number $a \in [0,1]$. $D[0,1]$ denotes the set of all interval numbers.

For interval numbers $D_1 = [a_1^-, b_1^+]$ and $D_2 = [a_2^-, b_2^+]$, we define

(1) r $\min(D_1, D_2)$ = r min ($[a_1^-, b_1^+], [a_2^-, b_2^+]$) = [$\min\{a_1^-, a_2^-\}$, $\min\{b_1^+, b_2^+\}$]

(2) r $\max(D_1, D_2)$ = r max ($[a_1^-, b_1^+], [a_2^-, b_2^+]$) = [max $\{a_1^-, a_2^-\}$, max $\{b_1^+, b_2^+\}$]

(3) $D_1 + D_2 = [\, a_1^- + a_2^- - a_1^-.a_2^-,\ b_1^+ + b_2^+ - b_1^+.b_2^+ \,]$

2.3 Definition: The interval-valued Q-fuzzy set A in V is define by

A= $\{ (x, [\mu_A^-(x,q), \mu_A^+(x,q)]) / x \in V\}$, where $\mu_A^-(x,q)$ & $\mu_A^+(x,q)$ are Q-fuzzy subsets of V such that $(x,q) \leq$ (x,q) for all $x \in V$ and $q \in$ Q.

2.4 Definition: By an interval -valued Q-fuzzy graph $G^* = (V,E)$ we mean a pair G=(A,B),where A=$[\mu_A^-, \mu_A^+]$ is an interval-valued Q-fuzzy set on V and B==$[\mu_B^-, \mu_B^+]$ is an interval-valued Q-fuzzy relation on E.

2.5 Definition : For a non- empty set G, we call a mapping A=(μ_A, γ_A):G × Q →D[0,1]× D[0,1] an interval –valued intuitionistic Q-fuzzy set if $\mu_A^+(x,q) + V_A^+(x,q) \leq \mathbf{1}$ *and* $\mu_A^-(x,q) + \gamma_A^-(x,q) \leq \mathbf{1}\, for\ all\ x \in G$, where the mapping

$$\mu_A(x,q) = [\mu_A^-(x,q),\ \mu_A^+(x,q)] : G \times Q \to D\,[0,1] \text{ and}$$

$$\gamma_A(x,q) = [\gamma_A^-(x,q),\ \gamma_A^+(x,q)] : G \times Q \to D\,[0,1]$$

are the degree of membership functions respectively. We use $\tilde{0}$ to denote the interval-valued fuzzy empty set and $\tilde{1}$ to denote the interval-valued fuzzy whole set in a set G, and we define $\tilde{0}(x,q) = [0,0]$ and $\tilde{1}(x,q) = [1,1]$, for all $X \in G$ and $q \in G$

2.6 Definition: If $G^* = (V,E)$ is a graph, then by an interval –valued intuitionistic Q-fuzzy relation B on a set E, we mean an interval –valued intuitionistic Q-fuzzy set such that

$$\mu_B(xy,q) \leq r\,\mathbf{min}\ (\ \mu_A(x,q),\ \mu_A(y,q)\ )$$

$$\gamma_B(xy,q) \geq r\,\mathbf{max}\ (\ \gamma_A(x,q),\ \gamma_A(y,q)\ )$$

for all $xy \in E$ and $q \in Q$.

3 .INTERVAL–VALUED INTUITIONISTIC Q-FUZZY GRAPHS

3.1 Definition: An Interval –valued intuitionistic Q-fuzzy graph with underlying set V is defined to be a pair G = (A,B) where

(i) The functions $\mu_A : V \times Q \to$ D[0,1] and $\gamma_A : V \times Q \to$ D[0,1] denote the degree of membership and non-membership of the element $X \in V$, respectively such that $\tilde{0} \leq$ $\mu_A(x,q)$+ $\gamma_A(x,q) \leq \tilde{1}$,for all $x \in V$ and $q \in Q$.

(ii) The functions μ_B :E⊆ $V \times V \times \quad \rightarrow$ D[0,1] & γ_B :E⊆ $V \times V \times \quad \rightarrow$ D[0,1]

and defined by $\mu_B(\{x,y\})q \leq r\, min\ (\ \mu_A(x,q).\ \ \mu_A(y,q)\ )$ and

$$\gamma_B(\{x,y\})q \geq r\ \max(\ \gamma_A(x,q),\ \ \gamma_A(y.q)\ )$$

such that $\tilde{0} \leq\ \ u_A(x, \quad + \gamma_A(x,q) \leq \tilde{1}$ for all $\{x,y\} \in E$ and $q \in G$.

We call A an interval –valued intuitionistic Q-fuzzy vertex set of V, B an interval –valued intuitionistic Q-fuzzy edge set of G, respectively. Note that B is a symmetric interval –valued intuitionistic Q-fuzzy relation on A .we use thethe notation xy for an element of E. Thus G=(A,B) is an interval –valued intuitionistic Q-fuzzy graph of G(V,E) if

$$\mu_B(xy,q) \leq r\, \boldsymbol{min}\ (\ \mu_A(x,q),\ \ \mu_A(y,q)\ \ )$$

$$\gamma_B(xy,q) \geq r\ \boldsymbol{max}\ (\ \gamma_A(x,q),\ \ \gamma_A(y,q)\ \ )$$

for all $xy \in E$ and $q \in Q$.

Example 3.2: Consider a graph $G^* = (V,E)$ such that V=$\{x, y,z\}$,E=$[xy, yz,zx\}$. Let 'A'be on IVIQFS of V and let B be on IVIQFS of E ⊆ $V \times V$ defined by

$$A = \langle\left(\frac{x}{[0.2,0.3]}, \frac{y}{.[0.1,0.4]}, \frac{z}{[0.3,0.5]}\right), \left(\frac{x}{[0.3,0.4]}, \frac{y}{.[0.2,0.6]}, \frac{z}{[0.1,0.7]}\right)\rangle$$

$$B = \langle\left(\frac{xy}{[0.03,0.2]}, \frac{yz}{.[0.04,0.05]}, \frac{zx}{[0.01,0.07]}\right), \left(\frac{xy}{[0.1,0.4]}, \frac{yz}{.[0.06,0.3]}, \frac{zx}{[0.07,0.3]}\right)\rangle$$

By routine computations, it is easy to see that G=(A,B) is a IVIQFG of G.

3.3 Definition: Let A= (μ_A,γ_A) and A'= $(\mu_A{}',\gamma_A{}'\ )$be a IVIQF subsets of V_1 and V_2 and B=(μ_B,γ_B) and B'=$(\ \mu_B{}', \gamma_B{}')$ be IVIQF of subset of $E_1 and\ E_2$ respectively .The Cartesian product of two IVIQFGS. G_1 and G_2 of the graphs G_1^* and G_2^* is denoted by $G_1 \times G_2\ = (A \times A', B \times B')$ and is defined as follows,

(i) $(\mu_A \times \mu_A{}')\ (x_1\,, x_2)_q =\ r\ \boldsymbol{min}\ (\ \mu_A(x_1,q),\ \mu_A{}'(x_2,q))$

$(\gamma_A \times\ \gamma_A{}')\ (x_1\,, x_2)_q =\ r\ \boldsymbol{max}\ \ (\gamma_A(x_1,q),\ \gamma_A{}'(x_2,q))$ for all $(x_1\,,x_2) \in V, q \in G$.

(ii) $(\ \mu_B \times \mu_B{}')\ ((x_1\,, x_2)(y_1\,, y_2))_q =\ \ r\ min\ (\ \mu_A(x,q), \mu_B{}'(x_2y_2,q))$

$(\ \gamma_B \times \gamma_B{}')\ ((x_1\,, x_2)(y_1\,, y_2))_q =\ \ r\ max\ (\gamma_A(x,q),\ \gamma_B{}'(x_2y_2,q))$

for all $x \in V_1$, for all $x_2y_2 \in E_2$

(iii) $(\mu_B \times \mu_B{}')\ ((x_1\,, z)(y_1\,, z))_q\ =\ r\ min\ (\mu_B(x_1y_1,q),\ \mu_A{}'(z,q))$

$(\gamma_B \times \gamma_B{}')\ \ ((x_1\,, z)(y_1\,, z))_q\ =\ r\ max\ (\gamma_B(x_1y_1,q),\ \ \gamma_A{}'(z,q))$

for all z ∈ V_2, for all $x_1y_1 \in E_1$.

Proposition 3.4: Let G_1 and G_2be the two interval –valued intuitionistic Q-fuzzy graphs. Then Cartesian product $G_1\ \times G_2$ is an interval –valued intuitionistic Q-fuzzy graphs.

Proof: Let $x \in\ V_1,\ x_2y_2 \in E_2$ then

$$(\mu_B \times \mu_B{}^{/})\ ((x\ ,x_2)(x\ ,y_2))_q = r\ \boldsymbol{min}\{(\ \mu_A(x,q), \mu_B{}^{/}(x_2y_2,q)\}$$
$$\leq\ r\ \min\{(\ \mu_A(x,q), rmin\ (\mu_A{}^{/}(x_2,q), \mu_A{}^{/}(y_2,q)\}$$
$$= r\ \min\{r\ \min\ (\ \mu_A(x,q), \mu_A{}^{/}(x_2,q)), rmin(\ \mu_A(x,q), (\ \mu_A{}^{/}(y_2,q))\}$$
$$= r\ \boldsymbol{min}\ \{(\ \mu_A \times \mu_A{}^{/})\ (x\ ,x_2)_q, (\ \mu_A \times \mu_A{}^{/})\ (x\ ,y_2)_q)\}$$

$$(\gamma_B \times \gamma_B{}^{/})\ ((x\ ,x_2)(x\ ,y_2))_q = r\ max\ \{(\ \gamma_A(x,q), \gamma_B{}^{/}(x_2y_2,q)\}$$
$$\geq\ r\ \max\{(\ \gamma_A(x,q), rmax\ (\gamma_A{}^{/}(x_2,q), \gamma_A{}^{/}(y_2,q)\}$$
$$= r\ \max\{r\ \max\ (\ \gamma_A(x,q), \gamma_A{}^{/}(x_2,q)), r\ \max\ (\ \gamma_A(x,q)\ , \gamma_A{}^{/}(y_2,q))\}$$
$$= r\ \boldsymbol{max}\ \{(\ \gamma_A \times\ \ \gamma_A{}^{/})\ (x\ ,x_2)_q, (\ \gamma_A \times\ \gamma_A{}^{/})\ (x\ ,y_2)_q\}$$

Let z ∈ $V_2,\ x_1y_1 \in E_1$ then

$$(\mu_B \times \mu_B{}^{/})\ ((x_1\ ,z)(y_1\ ,z))_q\ =\ r\ min\ (\mu_B(x_1y_1,q),\ \mu_A{}^{/}(z,q))$$
$$\leq r\ \min\{r\ min\ (\mu_A(x_1,q), \mu_A(y_1,q)),\ \mu_A{}^{/}(z,q)\}$$
$$= r\ \min\{r\ \min\ (\mu_A(x_1,q),\ \mu_A{}^{/}(z,q)), r\ \min\ (\mu_A(y_1,q),\ \mu_A{}^{/}(z,q))\}$$
$$= r\ min\ \{(\mu_A \times\ \mu_A{}^{/})\ (x_1,z)_q, (\mu_A \times \mu_A{}^{/})\ (y_1,z)_q\}$$
$$(\gamma_B \times \gamma_B{}^{/})\ ((x_1\ ,z)(y_1\ ,z))_q\ =\ r\ \boldsymbol{max}\ (\gamma_B(x_1y_1,q),\ \ \gamma_A{}^{/}(z,q))$$
$$\geq r\ \max\{r\ max\ (\gamma_A(x_1,q), \gamma_A(y_1,q)),\ \gamma_A{}^{/}(z,q)\}$$
$$= r\ \max\{r\ \max\ (\gamma_A(x_1,q),\ \gamma_A{}^{/}(z,q)), r\ \max\ (\gamma_A(y_1,q),\ \gamma_A{}^{/}(z,q))\}$$
$$= r\ max\ \{(\gamma_A \times\ \gamma_A{}^{/})\ (x_1,z)_q, (\gamma_A \times \gamma_A{}^{/})\ (y_1,z)_q\}$$

3.5 Definition: Let A= (μ_A,γ_A) and $A^{/}$= $(\ \mu_A{}^{/},\gamma_A{}^{/})$ be an IVIQF subsets of V_1 and V_2 and B= (μ_B,γ_B) and $B^{/}$= $(\mu_B{}^{/},\gamma_B{}^{/})$ be IVIQF of subset of $E_1 and\ E_2$ respectively .The Composition of two IVIQFGs G_1 and G_2 is denoted by $G_1[G_2\,] = (AoA^{/}, BoB^{/})$ and is defined as follows,

(i) $(\ \mu_A o\ \mu_A{}^{/})\ (x_1\ ,x_2)_q = r\ min\ (\mu_A(x_1,q),\ \mu_A{}^{/}(x_2,q))$

$(\ \gamma_A o\ \gamma_A{}^{/})\ (x_1\ ,x_2)_q = r\ max\ (\gamma_A(x_1,q),\ \gamma_A{}^{/}(x_2,q))$ for all $(x_1\ ,x_2)$ ∈V.

(ii) $(\ \mu_B o\ \mu_B{}^{/})\ ((x,x_2)(x,y_2))_q = r\ min\ (\mu_A(x,q),\ \mu_B{}^{/}(x_2y_2,q))$

$(\ \gamma_B o\ \gamma_B{}^{/})\ ((x,x_2)(x,y_2))_q = r\ max\ (\gamma_A(x,q),\ \gamma_B{}^{/}(x_2y_2,q))$

(iii) $(\ \mu_B o\ \mu_B{}^{/})\ ((x_1\ ,z)(y_1\ ,z))_q = r\ min\ (\mu_B(x_1y_1,q),\ \mu_A{}^{/}(z,q))$

$(\ \gamma_B o\ \gamma_B{}^{/})((x_1\ ,z)(y_1\ ,z))_q = r\ max\ (\gamma_B(x_1y_1,q),\ \ \gamma_A{}^{/}(z,q))$

(iv) $(\ \mu_B o\ \mu_B{}^{/})((x_1\ ,x_2)(y_1\ ,y_2))_q = r\ min\ (\ \mu_A{}^{/}(x_2,q),\ \mu_A{}^{/}(y_2,q), \mu_B(x_1y_1,q))$

$(\ \gamma_B o\ \gamma_B{}^{/})((x_1\ ,x_2)(y_1\ ,y_2))_q = r\ min\ (\ \gamma_A{}^{/}(x_2,q),\ \gamma_A{}^{/}(y_2,q), \gamma_B(x_1y_1,q))$

for all $(x_1\ x_2)(y_1\ y_2) \in E^{o}$-$E$.

Proposition 3.6: Let G_1 and G_2be the two interval –valued intuitionistic Q-fuzzy graphs. Then Composition of $G_1[G_2]$ is an interval –valued intuitionistic Q-fuzzy graphs.

Proof:

Let $x \in V_1,\ x_2y_2 \in$ E then

$$(\mu_B o\, \mu_B{}')\,((x,x_2)(x,y_2))_q = r\,min\,(\mu_A(x,q),\ \mu_B{}'(x_2y_2,q))$$

$$\leq r\min\ \{\mu_A(x,q), r\min\,(\mu_A{}'(x_2,q),\ \mu_A{}'(y_2,q))\}$$

$$= r\min\,\{r\,min\,(\mu_A(x,q)\,,\ \mu_A{}'(x_2,q))\,, r\,\mathbf{min}\,(\mu_A(x,q),\ \mu_A{}'(y_2,q))\}$$

$$= r\,\mathbf{min}\ \{(\mu_A o\, \mu_A{}')(x,x_2)\,, (\mu_A o\, \mu_A{}')(x,y_2)\}$$

$$(\gamma_B o\, \gamma_B{}')\,((x,x_2)(x,y_2))_q = r\,max\,(\gamma_A(x,q),\ \gamma_B{}'(x_2y_2,q))$$

$$\geq\ r\max\{\gamma_A(x,q), r\max\left(\gamma_A{}'(x_2,q),\ \gamma_A{}'(y_2,q)\right)\}$$

$$= r\,\mathbf{max}\ \{r\max\,(\gamma_A(x,q)\,,\ \gamma_A{}'(x_2,q))\,, r\,\mathbf{max}\,(\gamma_A(x,q),\ \gamma_A{}'(y_2,q))\}$$

$$= r\,\mathbf{max}\ \{(\gamma_A o\, \gamma_A{}')(x,x_2)\,, (\gamma_A o\, \gamma_A{}')(x,y_2)\}$$

Let $z \in V_2,\ x_1y_1 \in$ E, then

$$(\mu_B o\, \mu_B{}')\,((x_1\,,z)(y_1\,,z))_q = r\,min\,(\mu_B(x_1y_1,q), (\,\mu_A{}'(z,q))$$

$$\leq r\min\ \{rmin(\mu_A(x_1,q),\ \mu_A(y_1,q)),\ \mu_A{}'(z,q)\}$$

$$\leq r\min\ \{rmin(\mu_A(x_1,q),\ \mu_A{}'(z,q))\,, rmin(\mu_A(y_1,q),\ \mu_A{}'(z,q))\}$$

$$= r\,\mathbf{min}\,\{(\mu_A o\, \mu_A{}')\,(x_1\,,z)\,, (\mu_A o\, \mu_A{}')\,(y_1\,,z)\}$$

$$(\gamma_B o\, \gamma_B{}')\,((x_1\,,z)(y_1\,,z))_q = r\,max\,(\gamma_B(x_1y_1,q),\ \gamma_A{}'(z,q))$$

$$\geq r\,\mathbf{max}\ \{rmax(\gamma_A(x_1,q),\ \gamma_A(y_1,q)),\ \gamma_A{}'(z,q)\}$$

$$\geq r\,\mathbf{max}\ \{rmax(\gamma_A(x_1,q),\ \gamma_A{}'(z,q))\,, rmax(\gamma_A(y_1,q),\ \gamma_A{}'(z,q))\}$$

$$= r\,\mathbf{max}\{(\gamma_A o\, \gamma_A{}')\,(x_1\,,z)\,, (\gamma_A o\, \gamma_A{}')\,(y_1\,,z)\}$$

Let $(x_1\ x_2)(y_1\ y_2) \in E^o$-$E$, so $\qquad\qquad$ $, x_2 \neq y_2$. Then

$$(\mu_B o \qquad)\,((x_1\,,x_2)(y_1\,,y_2))_q = r\,min\,(\,\mu_A{}'(x_2,q),\ \mu_A{}'(y_2,q), \mu_B(x_1y_1,q))$$

$$\leq r\min\,(\,\mu_A{}'(x_2,q),\ \mu_A{}'(y_2,q)), r\min\,(\mu_A(x_1,q), \mu_A(y_1,q))$$

$$\leq r\min\,\{\,r\min\,(\mu_A(x_1,q),\ \mu_A{}'(x_2,q)), r\min\,(\mu_A(y_1,q),\ \mu_A{}'(y_2,q))\}$$

$$= r\min\{(\,\mu_A o\, \mu_A{}')(x_1,x_2)_q\,, (\mu_A o\, \mu_A{}')(y_1,y_2)_q\}$$

$$(\gamma_B o\, \gamma_B{}')((x_1\,,x_2)(y_1\,,y_2))_q = r\,max\,(\,\gamma_A{}'(x_2,q),\ \gamma_A{}'(y_2,q), \gamma_B(x_1y_1,q))$$

$$\geq r\,max\,(\,\gamma_A{}'(x_2,q),\ \gamma_A{}'(y_2,q)), r\,max\,(\gamma_A(x_1,q), \gamma_A(y_1,q))$$

4.CONCLUSION:

The interval valued fuzzy model give more precision, flexibility and compatibility to the system as computed to the classical and fuzzy models. It is known that fuzzy graph theory has numerous applications in Modern science and Engineering, especially in the field of information theory, neural networks, expert systems, cluster analysis, medical diagnosis, traffic engineering and control theory. In this paper, we introduce the notion of interval –valued intuitionistic Q-fuzzy graphs and describe various methods of their construction. We also present the concept of interval-valued intuitionistic Q-fuzzy regular graphs.

REFERENCES

[1] M. Akram and W.A. Dudek, Interval-valued fuzzy graphs, Computers and Mathematicswith Applications, 61 (2011) 289-299.

[2] M. Akram and KH. Dar, Generalized fuzzy K -algebras, VDM Verlag, 2010, pp.288,ISBN 978-3-639-27095-2.

[3] KT. Atanassov, Intuitionistic fuzzy fets: Theory and applications, Studies in fuzzinessand soft computing, Heidelberg, New York, Physica-Verl., 1999.

[4] J.N. Mordeson and C.S. Peng, Operations on fuzzy graphs, Information Sciences 79(1994) 159-170.

[5] J.N. Mordeson and P.S. Nair, Fuzzy graphs and fuzzy hypergraphs, Physica Verlag, Heidelberg1998; Second Edition 2001.

[6] T. Gerstenkorn and J. Manko, Bifuzzy probabilistic sets, Fuzzy Sets and Systems 71(1995), 207-214.

[7] A. Shannon, KT. Atanassov, A first step to a theory of the intuitionistic fuzzy graphs,Proceeding of FUBEST (D. Lakov, Ed.), Sofia, (1994) 59-61.10

[8] A. Rosenfeld, Fuzzy graphs, Fuzzy Sets and their Applications(L.A.Zadeh, K.S.Fu,M.Shimura, Eds.), Academic Press, New York, (1975) 77-95.

[9] A.Solairaju and R.Nagarajan ,A New Structure and Construction of Q-fuzzy groups" Advances in Fuzzy Mathematics Vol.4,No.1(2009),23-29.

[10] L.A. Zadeh, Similarity relations and fuzzy orderings, Information Sciences3(2)(1971)177- 200.

[11] L.A. Zadeh, The concept of a linguisistic variable and its application to approximate reasoning, Information Sci. 8 (1975)199-249.

AUTHOR'S DETAIL:

Dr. R.NAGARAJAN has been working as Associate Professor and Head of Mathematics in J.J.College of Engineering & technology,Trichy. He has 16 years of experience in the field of Teaching. He has completed his M.Sc., from Bharathidasan University, Trichy M.Phil in the field of Minimal graphoidal cover of a graph from Alagappa University, Karaikudi. He Received his Ph.D degree in the field of Fuzzy Techniques in Algebra from Bharathidasan University, ,Trichy. He has Published more than 50 research articles in International Journals and 4 in National Journals. His area of interests are Fuzzy Algebraic Structures, Fuzzy Topological Structures, Fuzzy Decision making and Fuzzy Optimizations.

Fuzzy Soft Matrix and Multi Criteria in Decision Making based on Weighted T-Norm Operators

Md. Jalilul Islam Mondal*, Tapan Kumar Roy*

* Department of Mathematics, Bengal Engineering and Science University ,
Shibpur , Howrah- 711103

ABSTRACT

The purpose of this paper is to put forward the notion of fuzzy soft matrix theory and some basic results. In this paper , we define fuzzy soft matrices and some new operators on weighted t- norms with properties . Lastly we have given an application in decision making based on different operators of weighted t-norms.

Key words – Soft sets, fuzzy soft matrices , operators of weighted t-norms.

1. INTRODUCTION

Most of our traditional tools for formal modeling, reasoning, and computing are crisp, deterministic, and precise in character. However, in real life, there are many complicated problems in engineering, economics, environment, social sciences medical sciences etc. that involve data which are not all always crisp, precise and deterministic in character because of various uncertainties typical problems. Such uncertainties are being dealing with the help of the theories, like theory of probability, theory of fuzzy sets, theory of intuitionistic fuzzy sets, theory of interval mathematics and theory of rough sets etc. Molodtsov [1] also described the concept of "Soft Set Theory" having parameterization tools for dealing with uncertainties. Researchers on soft set theory have received much attention in recent years. Maji and Roy [3,4] first introduced soft set into decision making problems. Maji et al.[2] introduced the concept of fuzzy soft sets by combining soft sets and fuzzy sets. Cagman and Enginoglu [5] defined soft matrices which were a matrix representation of the soft sets and constructed a soft max-min decision making method. Cagman and Enginoglu [6] defined fuzzy soft matrices and constructed a decision making problem . Borah et al.[7] extended fuzzy soft matrix theory and its application. Maji and Roy [8] presented a novel method of object from an imprecise multi-observer data to deal with decision making based on fuzzy soft sets. Majumdar and samanta [9] generalized the concept of fuzzy soft sets.In this paper , we have introduced some operators of fuzzy soft matrix on the basis of weighted t-norms . We have also discussed their properties . Finally we have given an application in decision making problem on the basis of weighted t-norms operators .

2. DEFINITION AND PRELIMINARIES:

2.1 Soft set [1] Let U be an initial universe , P(U) be the power set of U , E be the set of all parameters and A⊆E. A soft set (f_A,E) on the universe U is defined by the set of order pairs

$$(f_A, E) = \{(e\ ,\ f_A(e)) : e \in E\ ,\ f_A(e) \in P(U)\ \}$$

$$\text{where } f_A : E \rightarrow P(U) \text{ such that } f_A(e) = \phi \text{ if } e \notin A.$$

Here f_A is called an approximate function of the soft set (f_A,E). The set f_A(e) is called e-approximate value set or e-approximate set which consists of related objects of the parameter e ∈ E.

Example 1 let U = { u_1, u_2, u_3, u_3} be a set of four balls and E = { white(e_1), red (e_2) ,blue (e_3) } be a set of parameters. If A ={e_1 ,e_2 }⊆ E. Let $f_A(e_1)$= {u_1 ,u_2 ,u_3 } and $f_A(e_2)$= { , u_1 u_2 , u_3 , u_4} , then we write the soft set (f_A,E)= {(e_1,{ u_1 , u_2 , u_3 }), (e_2,{ u_1 , u_2 , u_3 , u_4})} over U which describe the "colour of the balls" which Mr. X is going to buy.

2.2 Fuzzy set [2] A Fuzzy Set (FS) in the universal set U is defined as A= { (x , μ_A(x)) | x ∈ U } where μ_A : U → [0,1] is a mapping called membership function of the fuzzy set A .

Example 2. Consider the example 1, here we can not express with only two real numbers 0 and 1, we can characterized it by a membership function instead of crisp number 0 and 1, which associate with each element a real number in the interval [0,1].Then

(f_A,E) = { $f_A(e_1)$ = { (u_1,.7) ,(u_2,.5) ,(u_3,.4) }, $f_A(e_2)$ = { (u_1,.5) , (u_2,.1) , (u_3,.5) ,(u_4,.2) } } is

the fuzzy soft set representing the "colour of the balls" which Mr. X is going to buy.

2.3 Fuzzy Soft Matrices (FSM) [5] Let (, E) be fuzzy soft set over U. Then a subset of U x E is uniquely defined by

$$R_A = \{ (u, e) : e \in A \ , u \in f_A(e) \},$$

which is called relation form of (f_A, E) .

The characteristic function of R_A is written by

μ_{R_A} : U x E → [0 , 1] , where $\mu_{R_A}(u , e) \in [0,1]$ is the membership value of u ∈ for each e ∈U.

If $\mu_{ij} = \mu_{R_A}(u_i, e_j)$, we can define a matrix

$$[\mu_{ij}]_{mXn} = \begin{bmatrix} \mu_{11} & \mu_{12} & \cdots & \mu_{1n} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \mu_{m1} & \mu_{m2} & \cdots & \mu_{mn} \end{bmatrix}$$

which is called an m x n soft matrix of the soft set (f_A,E) over U.

Therefore we can say that a fuzzy soft set (,E) is uniquely characterized by the matrix $[\mu_{ij}]_{mXn}$ and both concepts are interchangeable.

Example 3. Assume that U = { u_1 , u_2 , u_3 , u_4, u_5, u_6} is a universal set and E = { e_1 , e_2 , e_3, e_4} is a set of all parameters. If A⊆ E = { e_1 , e_2 , e_4} and

$f_A(e_1)$= { (u_1 ,.7), (u_2,.4) , (u_3,.6) , (u_4,.1),(u_5,.6), (u_6,.5 }

$f_A(e_2)$= { (u_1,.3) , (u_2,.5) , (u_3,.7) , (u_4,.3) ,(u_5,.7), (u_6,.1)}

$f_A(e_4)$= { (u_1,.4) , (u_2,.2) , (u_3,.5) , (u_4,.6),(u_5,.7), (u_6,.3) }

Then the fuzzy soft set (f_A,E) is a parameterized family { $f_A(e_1)$, $f_A(e_2)$, $f_A(e_3)$} of all fuzzy sets over U.

Hence the fuzzy soft matrix $[\mu_{ij}]$ can be written as

$$[\mu_{ij}] = \begin{bmatrix} .7 & .3 & 0 & .4 \\ .4 & .5 & 0 & .2 \\ .6 & .7 & 0 & .5 \\ .1 & .3 & 0 & .6 \\ .6 & .7 & 0 & .7 \\ .5 & 1 & 0 & .3 \end{bmatrix}$$

2.4. Zero Fuzzy Soft Matrix [6] Let $[a_{ij}]$ $\in$F $SM_{m X n}$. Then $[a_{ij}]$ is called a Zero Fuzzy Soft Matrix denoted by [0], if $a_{ij} = 0$ for all i and j.

2.5. Universal Fuzzy Soft Matrix [6] Let $[a_{ij}]$ $\in$ $FSM_{m X n}$. Then $[a_{ij}]$ is called a Universal Fuzzy Soft Matrix denoted by [1], if $a_{ij} = 1$ for all i and j.

2.6. Fuzzy Soft Sub Matrix [6] Let $[a_{ij}], [b_{ij}]$ $\in$F $SM_{m X n}$. Then

$[a_{ij}]$ is said to be a Fuzzy Soft Sub Matrix of $[b_{ij}]$ denotedby $[a_{ij}] \tilde{\subseteq} [b_{ij}]$ if $a_{ij} \leq b_{ij}$ for all i and j .

2.7. Union of Fuzzy Soft Matrices [6] Let $[a_{ij}]$, $[b_{ij}]$ $\in$F $SM_{m X n}$. Then

Union of $[a_{ij}]$ and $[b_{ij}]$, denoted by $[a_{ij}] \tilde{\cup} [b_{ij}]$ is defined as

$[a_{ij}] \tilde{\cup} [b_{ij}$ =max $\{a_{ij}, b_{ij}\}$ for all i and j

2.8. Intersection of Fuzzy Soft Matrices [6] Let $[a_{ij}], [b_{ij}]$ $\in$F $SM_{m X n}$. Then

Intersection of $[a_{ij}]$ and $[b_{ij}]$, denoted by $[a_{ij}] \tilde{\cap} [b_{ij}]$ is defined as

$[a_{ij}] \tilde{\cap} [b_{ij}]$ =min $\{a_{ij}, b_{ij}\}$ for all i and j

2.9. Compliment Fuzzy Soft Matrix [6] Let $[a_{ij}]$ $\in$ $FSM_{m X n}$. Then Complement of Fuzzy Soft Matrix , denoted by $[a_{ij}]^0$ is defined as $[a_{ij}]^0 = 1 - a_{ij}$ for all i and j.

2.10. Fuzzy Soft Equal Matrices [6] Let $[a_{ij}], [b_{ij}]$ $\in$F $SM_{m X n}$. Then

$[a_{ij}]$ and $[b_{ij}]$ are said to be Fuzzy Soft Equal Matrices , denoted by $[a_{ij}] = [b_{ij}]$ if $a_{ij} = b_{ij}$ for all i and j.

Proposition1. Let $[a_{ij}] \in FSM_{m X n}$. Then

i) $[[a_{ij}]^0]^0 = [a_{ij}]$ iv) $[a_{ij}] \tilde{\cap} [a_{ij}] = [a_{ij}]$

ii) $[a_{ij}] \tilde{\subseteq} [a_{ij}]$ v) $a_{ij}] \tilde{\cup} [0] = [a_{ij}]$

iii) $[a_{ij}] \tilde{\cup} [a_{ij}] = [a_{ij}]$ vi) $[a_{ij}] \tilde{\cap} [0] = [0]$

Proposition2. Let $[a_{ij}], [b_{ij}], [c_{ij}]$ $\in$ $SM_{m X n}$. Then

i) $[a_{ij}] = [b_{ij}]$ and $[b_{ij}] = [c_{ij}]$ $\Rightarrow [a_{ij}] = [c_{ij}]$

ii) $a_{ij}] \subseteq [b_{ij}]$ and $[b_{ij}] \tilde{\subseteq} [c_{ij}]$ $\Rightarrow [a_{ij}] = [c_{ij}]$

Proposition3. Let $[a_{ij}], [b_{ij}], [c_{ij}]$ $\in$F SM$_{m\,X\,n}$. Then

i) $[a_{ij}] \tilde{\cup} ([b_{ij}] \tilde{\cap} [c_{ij}]) = ([a_{ij}] \tilde{\cup} [b_{ij}]) \tilde{\cap} ([a_{ij}] \tilde{\cup} [c_{ij}])$

ii) $[a_{ij}] \tilde{\cap} ([b_{ij}] \tilde{\cup} [c_{ij}]) = ([a_{ij}] \tilde{\cap} [b_{ij}]) \tilde{\cup} ([a_{ij}] \tilde{\cap} [c_{ij}])$

2.11. Fuzzy Soft Rectangular Matrix [7] Let $[a_{ij}]$ $\in$ F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Rectangular Matrix if m $\neq$ n .

2.12. Fuzzy Soft Square Matrix [7] Let $[a_{ij}]$ $\in$ F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Square Matrix if m = n .

2.13. Fuzzy Soft Row Matrix [7] Let $[a_{ij}]$ $\in$F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Row Matrix if m = 1 .

2.14. Fuzzy Soft Column Matrix [7] Let $[a_{ij}]$ $\in$F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Column Matrix if n = 1 .

2.15. Fuzzy Soft Diagonal Matrix [7] Let $[a_{ij}]$ $\in$F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Diagonal Matrix if m = n and $a_{ij} = 0$ for all i $\neq$ j .

2.16. Fuzzy Soft Upper Triangular Matrix [7] Let $[a_{ij}]$ $\in$ F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Upper Triangular Matrix if m = n and $a_{ij} = 0$ for all i> j .

2.17. Fuzzy Soft Lower Triangular Matrix [7] Let $[a_{ij}]$ $\in$ F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Lower Triangular Matrix if m = n and $a_{ij} = 0$ for all i< j .

2.18. Fuzzy Soft Triangular Matrix [7] Let $[a_{ij}]$ $\in$ F SM$_{m\,X\,n}$. Then $[a_{ij}]$ is said to be a Fuzzy Soft Triangular Matrix if is either fuzzy soft lower or fuzzy soft upper triangular matrix for all i and j .

2.19. t-Norm [10]: Let T : [0,1] x [0,1] be a function satisfying the following axioms:

i) T(a , 1) = a , $\forall$ a $\in$ [0,1] (Identity)

ii) T(a, b) = T(b ,a) , $\forall$ a ,b $\in$ [0,1] (Commutativity)

iii) if $b_1 \leq b_2$, then T(a, b_1) $\leq$ T(a, b_2) , $\forall$ a , b_1 , b_2 $\in$ [0,1] (Monotonicty)

iv) T (a, T(b,c)) = T(T (a,b) , c) , $\forall$ a ,b $\in$ [0,1] (Associativity)

Then T is called t-norm.

A t-norm is said to be continuous if T is continuous function in [0,1]. An example of continuous t- Norm is a b .

N.B. :The functions used for intersection of fuzzy sets are called t-norms.

2.20. t-Conorm[10]: Let S : [0,1] x [0,1] be a function satisfying the following axioms:

i) $S(a , 0) = a , \forall a \in [0,1]$ (Identity)

ii) $S(a,b) = S(b,a) , \forall a ,b \in [0,1]$ (Commutativity)

iii) if $b_1 \leq b_2$, then $S(a, b_1) \leq S(a, b_2) , \forall a , b_1 , b_2 \in [0,1]$ (Monotonicity)

iv) $S (a, S(b,c)) = S(S (a,b) , c) \forall a ,b \in [0,1]$ (Associativity)

Then S is called t-conorm.

A t-conorm is said to be continuous if S is continuous function in [0,1].

N.B. :The functions used for union of fuzzy sets are called t-conorms.

An example of continuous t- Conorm is a + b - a .b .

2.21. Union of Fuzzy Soft Matrices on t-norm: Let $[a_{ij}] , [b_{ij}] \notin SM_{m X n}$.Then

Union of Fuzzy Soft Matrices $[a_{ij}]$ and $[b_{ij}]$ on t-norm is defined by

$[a_{ij}] \tilde{\cup} [b_{ij}] = [a_{ij} + b_{ij} - a_{ij} . b_{ij}]$ for all i and j.

2.22. Intersection of Fuzzy Soft Matrices on t-norm: Let$[a_{ij}]$,$[b_{ij}] \in FSM_{m X n}$.Then

Intersection of Fuzzy Soft Matrices $[a_{ij}]$ and $[b_{ij}]$ on t-norm is defined by

$[a_{ij}] \tilde{\cap} [b_{ij}] = [a_{ij} . b_{ij}]$ for all i and j.

Proposition4. Let $[a_{ij}] , [b_{ij}] , [c_{ij}] \in FSM_{m X n}$. Then

i) $[0] =$ iii) $[a_{ij}] \tilde{\cup} [b_{ij}] = [b_{ij}] \tilde{\cup} [a_{ij}]$

ii) $[1] = [1]$ iv) $([a_{ij}] \tilde{\cup}$) $[c_{ij}] =$ $\tilde{\cup}$ ( )

Proposition5. Let $[a_{ij}] , [b_{ij}] ,[c_{ij}] \in FSM_{m X n}$. Then

i) $[a_{ij}] \tilde{\cap} [0] =$ iii) $[a_{ij}] \tilde{\cap} [b_{ij}] = [b_{ij}] \tilde{\cap} [a_{ij}]$

ii) $[a_{ij}] \tilde{\cap} [1] =$ iv) $([a_{ij}] \tilde{\cap} [b_{ij}])$ $[c_{ij}] = [a_{ij}] \tilde{\cap} ([b_{ij}] \tilde{\cap} [c_{ij}])$

Proposition6. Let , $[b_{ij}]$ $FSM_{m X n}$. Then

De Morgan's type results are true :

i) $([a_{ij}] \tilde{\cup} [b_{ij}])^0 = [a_{ij}]^0 \tilde{\cap} [b_{ij}]^0$

ii) $([a_{ij}] \tilde{\cap} [b_{ij}])^0 = [a_{ij}]^0 \tilde{\cup} [b_{ij}]^0$

Proof: for all i and j ,

i) $([a_{ij}]\ \tilde{\cup}\ [b_{ij}])^0 = [a_{ij}\ -b_{ij}\ -\ a_{ij}.b_{ij}\ ]^0$

$$= [\ 1 - (a_{ij} - b_{ij} -\ a_{ij}.b_{ij})\ ]$$

$$= [\ 1 - a_{ij} - b_{ij} -\ a_{ij}.b_{ij})\ ]$$

$$= [\ (1 - a_{ij})\ (1 - b_{ij})\ ]$$

$$= [\ 1 - a_{ij}\ ]\ \tilde{\cap}\ [1 - b_{ij}\ ]$$

$$= [a_{ij}]^0\ \tilde{\cap}\ [b_{ij}]^0 \qquad \square$$

ii) Similar proof for ii).

2.23. Scalar Multiplication of Fuzzy Soft Matrix : Let $[a_{ij}]$ ∈F $SM_{m\ X\ n}$. Then

Scalar Multiplication of Fuzzy Soft Matrix $[a_{ij}]$by a scalar k denoted by k$[a_{ij}]$is defined as k $[a_{ij}] = [\ \mathrm{k}a_{ij}]$, $0 \leq \mathrm{k} \leq 1$.

Proposition7. Let $[a_{ij}]$ ∈F $SM_{m\ X\ n}$ and s and t are two scalars such that $0 \leq s, t \leq 1$. Then

i) $s(t[a_{ij}]) = (st)\,[a_{ij}]$

ii) $s \leq t \Rightarrow s[a_{ij}]\ \tilde{\subseteq}\ t\,[a_{ij}]$

iii) $[a_{ij}]\ \tilde{\subseteq}\ [b_{ij}] \Rightarrow s[a_{ij}]\ \tilde{\subseteq}\ s[b_{ij}]$

2.24. Three Important Operators of t- Norms[11] :

i) **Minimum Operator :** $T_M(\ \mu_1, \mu_2, \ldots\ldots, \mu_n) = \min(\ \mu_1, \mu_2, \ldots\ldots, \mu_n)$

ii) **Product Operator :** $T_P(\ \mu_1, \mu_2, \ldots\ldots, \mu_n) = \prod_{i=1}^{n} \mu_i$

iii) **Operator Lukasiewicz t-norm (Bounded t-norm) :**

$T_L(\ \mu_1, \mu_2, \ldots\ldots, \mu_n) = \max\ (\ \sum_{i=1}^{n} \mu_i\ - n + 1\ , 0\ )$

Example4. Let $[a_{ij}]$, $[b_{ij}]$ ∈ $FSM_{3\ X3}$ where

$$[a_{ij}] = \begin{bmatrix} .3 & .2 & .6 \\ .1 & .7 & .5 \\ .3 & .4 & .6 \end{bmatrix} \text{ and } [b_{ij}] = \begin{bmatrix} .5 & .7 & .6 \\ .5 & .6 & .3 \\ .3 & .4 & .3 \end{bmatrix} .\ \text{Then}$$

$$T_M(\ [a_{ij}]\ , [b_{ij}]\ ) = \begin{bmatrix} .3 & .2 & .6 \\ .1 & .6 & .3 \\ .3 & .4 & .3 \end{bmatrix}$$

$$T_P([a_{ij}], [b_{ij}])\ = \begin{bmatrix} .15 & .14 & .36 \\ .5 & .42 & .15 \\ .09 & .16 & .18 \end{bmatrix}$$

$$T_L(\ [a_{ij}]\ , [b_{ij}]\ ) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

2.25. Arithmetic Mean (A.M.) of Fuzzy Soft Matrix : Let $\tilde{A} = [a_{ij}] \in$ F $\mathrm{SM}_{m\,X\,n}$. Then Arithmetic Mean of Fuzzy Soft Matrix of membership value denoted by $\tilde{A}_{AM}$ is defined as $\tilde{A}_{AM} = \frac{\sum_{j=1}^{n} \mu_{ij}^{\tilde{A}}}{n}$.

2.26. Three Important t- Norm Operators With Weights :

i) **Minimum Operator With Weight :** $T_M^W(\mu_1 ; w_1 , \mu_2 ; w_2 ,\ldots\ldots, \mu_n ; w_n) = \min \{ 1 - w_1(1 - \mu_1), 1 - w_2(1 - \mu_2), \ldots\ldots, 1 - w_n(1 - \mu_n) \}$

ii) **Product Operator With Weight :** $T_P^W(\mu_1 ; w_1 , \mu_2 ; w_2 ,\ldots\ldots, \mu_n ; w_n) = \prod_{i=1}^{n} \{ 1 - w_i(1 - \mu_i) \}$

iii) Operator of Lukasiewicz t- norm With Weight (Bounded t-norm With Weight) : $T_L^W(\mu_1 ; w_1 , \mu_2 ; w_2 ,\ldots\ldots, \mu_n ; w_n) = \max (\sum_{i=1}^{n} 1 - w_i(1 - \mu_i) - n + 1 , 0)$

Proposition8. Let $[a_{ij}] \in \mathrm{FSM}_{m\,X\,n}$ and w_1 be the weight . Then

i) $= [a_{ij}]$ iv) $= [a_{ij}]$

ii) $= [a_{ij}]$ v) $= [a_{ij}]$

iii) $[a_{ij}] \widetilde{\cap}_{T_L^w} [a_{ij}] = [a_{ij}]$ vi) $[a_{ij}] \widetilde{\cap}_{T_L^w} [1] = [a_{ij}]$

vii) $[a_{ij}] \widetilde{\cap}_{T_M^w} [0] = [0]$ viii) $[a_{ij}] \widetilde{\cap}_{T_P^w} [0] = [0]$

ix) $[a_{ij}] \widetilde{\cap}_{T_L^w} [0] = [0]$

Proof :

i) $[a_{ij}] \widetilde{\cap}_{T_M^w} [a_{ij}] = [\min \{ 1 - w_1(1 - a_{ij}), 1 - w_1(1 - a_{ij}) \}]$

$= [1 - w_1(1 - a_{ij})]$

$= [a_{ij}]$ □

Similar proofs for others.

Proposition9. Let $[a_{ij}], [b_{ij}] \in \mathrm{FSM}_{m\,X\,n}$ and w_1 , w_2 be the weights . Then

i) $[a_{ij}] \widetilde{\cap}_{T_M^w} [b_{ij}] = [b_{ij}] \widetilde{\cap}_{T_M^w} [a_{ij}]$

ii) $[a_{ij}] \widetilde{\cap}_{T_P^w} [b_{ij}] = [b_{ij}] \widetilde{\cap}_{T_P^w} [a_{ij}]$

iii) $[a_{ij}] \widetilde{\cap}_{T_L^w} [b_{ij}] = [b_{ij}] \widetilde{\cap}_{T_L^w} [a_{ij}]$

Proof : Straight forward from definition .

Proposition10. Let $[a_{ij}],[b_{ij}],[c_{ij}]$ $\in$FSM$_{m\,X\,n}$ and w_1 , w_2 , w_3 be their respective weights . Then

i) $([a_{ij}]\ \tilde{\cap}_{T_M^w}[b_{ij}])\tilde{\cap}_{T_M^w}\ [c_{ij}]=[a_{ij}]\tilde{\cap}_{T_M^w}([b_{ij}]\tilde{\cap}_{T_M^w}[c_{ij}])$

ii) $([a_{ij}]\ \tilde{\cap}_{T_P^w}[b_{ij}])\tilde{\cap}_{T_P^w}\ [c_{ij}]=[a_{ij}]\tilde{\cap}_{T_P^w}([b_{ij}]\tilde{\cap}_{T_P^w}[c_{ij}])$

iii) $([a_{ij}]\ \tilde{\cap}_{T_L^w}[b_{ij}])\tilde{\cap}_{T_L^w}\ [c_{ij}]=[a_{ij}]\tilde{\cap}_{T_L^w}([b_{ij}]\tilde{\cap}_{T_L^w}[c_{ij}])$

Proof :

$$([a_{ij}]\ \tilde{\cap}_{T_M^w}[b_{ij}])\tilde{\cap}_{T_M^w}\ [c_{ij}]$$

$$=\min\{\,1-w_1(1-\ a_{ij})\ ,\ 1-w_2(1-\ b_{ij})\}\ \tilde{\cap}_{T_M^w}\{1-w_3(1-\ c_{ij})\}$$

$$=\min\{\,1-w_1(1-\ a_{ij})\ ,\ 1-w_2(1-\ b_{ij}),1-w_3(1-\ c_{ij})\}$$

$$=\{\,1-w_1(1-\ a_{ij})\}\ \tilde{\cap}_{T_M^w}\min\{\,1-w_2(1-\ b_{ij}),1-w_3(1-\ c_{ij})\}$$

$$=[a_{ij}]\tilde{\cap}_{T_M^w}([b_{ij}]\tilde{\cap}_{T_M^w}[c_{ij}])$$

Similar proof for others.

3. FUZZY SOFT MATRICES IN DECISION MAKING BASED ON WEIGHTED T– NORMS

In this section , we put forward fuzzy soft matrices in decision making by using different operators of weighted t- norms.

Input: Fuzzy soft set of m objects , each of which has n parameters.

Output: An optimum result .

ALGORITHM

Step- 1: Choose the set of parameters.

Step -2: Construct the fuzzy soft matrix for the set of parameters.

Step- 3: Compute the arithmetic mean of membership value of fuz A_{AM} of natrix as different weighted t-norm ope A_{AM}^{w} .

Step-4: Choose the object with highest membership value.

Example 5.Suppose the management of a company established an annual university undergraduate scholarship to support high school students with excellent performance in science (Mathematics, Physics , Chemistry) . Suppose s_1, s_2, s_3, s_4, s_5 e five best students of different universities apply for the scholarship such that U = $\{\,s_1, s_2, s_3, s_4, s_5\}$ and E = $\{\ e_1$ tics) , e_2(Physics)

e_3 (Chemistry) } be the set of parameters . Suppose three Officers Mr. A , Mr. B and Mr. C of that company decıde that preference will be given on Mathematics .So .8 , .1 , .1 are given weights on Mathematics, Physics , Chemistry respectively and the following fuzzy soft matrices are constructed on the basis of the parameters as follows :

$$A = \begin{bmatrix} .8 & .9 & .8 \\ .7 & .8 & .4 \\ .9 & .6 & .7 \\ .5 & .3 & .5 \\ .9 & .6 & .7 \end{bmatrix}, B = \begin{bmatrix} .8 & .7 & .6 \\ .9 & .4 & .5 \\ .8 & .8 & .7 \\ .6 & .4 & .7 \\ .7 & .5 & .7 \end{bmatrix} \text{ and } C = \begin{bmatrix} .9 & .5 & .9 \\ .6 & .5 & .6 \\ .5 & .6 & .8 \\ .7 & .8 & .6 \\ .9 & .6 & .8 \end{bmatrix}$$

$$T_M^W = \begin{bmatrix} .84 & .95 & .96 \\ .68 & .94 & .94 \\ .6 & .96 & .97 \\ .6 & .93 & .95 \\ .76 & .95 & .97 \end{bmatrix} \text{ and } T_{M(AM)}^W = \begin{bmatrix} .92 \\ .85 \\ .84 \\ .82 \\ .89 \end{bmatrix} \cdots\cdots\cdots\cdots(3.1)$$

$$T_P^W = \begin{bmatrix} .649152 & .912285 & .931392 \\ .475456 & .87514 & .85728 \\ .46368 & .903168 & .922082 \\ .31008 & .856716 & .88464 \\ .778688 & .87552 & .922082 \end{bmatrix} \quad \text{and}$$

$$T_{P(AM)}^W) = \begin{bmatrix} .830943 \\ .735959 \\ .772521 \\ .683812 \\ .858763 \end{bmatrix} \cdots\cdots\cdots\cdots(3.2)$$

$$T_L^W = \begin{bmatrix} .2 & 1 & .2 \\ 0 & 0 & 0 \\ .2 & .3 & 1 \\ 0 & 0 & 0 \\ .2 & 0 & .2 \end{bmatrix} \text{ and } T_{L(AM)}^W = \begin{bmatrix} .167 \\ 0 \\ .2 \\ 0 \\ .133 \end{bmatrix} \cdots\cdots\cdots\cdots (3.3)$$

From the above result (3.1) ,it is obvious that s_1 student ; from (3.2) , $s_5$student and from (3.3) , s_3 student will be selected for the scholarship for their highest membership scores.

CONCLUSION

In this paper ,we proposed fuzzy soft matrices and defined different types of fuzzy soft matrices . We have given some definitions on t-norm operators with weight and their properties . Some of the properties have been proved. Finally , we extend our approach on weighted t-norm operators in application of decision making problems. It is obvious from the results that decisions are different for different methods on same application. This method can also be applied on other decision making problems with uncertain parameters.

REFERENCES

[1]. D. Molodtsov , Soft set theory – first result, Computers and Mathematics with Applications 37(1999) 19-31

[2] P. K. Maji, R. Biswas and A. R. Roy, "Fuzzy Soft Sets", Journal of Fuzzy Mathematics , Vol 9 , no.3 , (2001), pp.589 – 602.

[3]P.K.Maji , R. Biswas and A.R.Roy, An application of soft sets in a decision making problems, Computer and Mathematics with Applications 44(2002) 1077-1083

[4]P.K.Maji , R. Biswas and A.R.Roy, Soft Set Theory ,Computer and Mathematics with Applications 45(2003) 555-562

[5]. Naim Cagman , Serdar Enginoglu , Soft matrix theory and its decision making, Computers and Mathematics with Applications 59(2010)3308-3314

[6]. N. Cagman and S. Enginoglu , Fuzzy soft matrix theory and its application in decision making, Iranian Journal of Fuzzy Systems, vol.9, No. 1(2012)109-119

[7] Manas Jyoti Borah, Tridiv Jyoti Neog, Dusmanta Kumar Sut, Fuzzy soft matrix theory and its decision making , IJMER, vol.2 ,issue2 March-Apr , (2012) pp.121-127.

[8] P.K.Maji , A.R.Roy, A fuzzy soft set theoretic approach to decision making problems ,
Journal of Computational and Applied Mathematics 203(2007) 412 - 418

[9] P. Majumdar , S.K.Samanta ,Generalized fuzzy soft sets, Computers and Mathematics with Applications 59(2010)1425-1432

[10] James J. Buckley, Esfandiar Eslami , An Introduction to Fuzzy Logic and Fuzzy Sets , Physica-Verlag , Heidelberg ,New York(2002)

[11] Md. Jalilul Islam Mondal , Tapan Kumar Roy ,Theory of Fuzzy Soft Matrix and its Multi Criteria in Decision Making Based on Three Basic t-Norm Operators ,IJIRSET, Vol.2 , issue 10 , (2013) 5715-5723

(α, β) -Fuzzy Soft Int-Groups Over Fuzzy Soft Interior Ideals

R. Nagarajan*

* Associate Professor, Department of Mathematics, J. J College of Engineering &Technology, Tiruchirappalli-09

ABSTRACT

The aim of the paper is to lay a foundation for providing a soft fuzzy algebraic tool in considering many problems that contain uncertainties. In order to provide these soft fuzzy algebraic structures, the notion of (α, β) -fuzzy soft int-groups which is a generalization of that fuzzy soft groups is provided. By introducing the notion soft fuzzy cosets, soft fuzzy quotient groups based on (α, β) -fuzzy soft interior ideals are established. Finally , isomorphism theorems of (α, β) -fuzzy soft int-groups related to invariant fuzzy soft sets are discussed.

KEY WORDS: soft set, fuzzy set, fuzzy soft int-group, fuzzy soft interior ideal, soft fuzzy coset, soft fuzzy quotient group, invariant fuzzy soft set, extended image set.

1. INTRODUCTION:

The notion of fuzzy set was introduced by L.A.Zadeh[23], and since then this concept has been applied to various algebraic structure. Later several authors such as Booth[5] and Satyanarayana[20] studied the ideal theory of near-rings. Molodtsov[14] initiated the concept of soft sets that is free from the difficulties that have troubled the usual theoretical approaches. Molodtsov pointed out several directions for the applications of soft sets. Maji et.al [15]gave the operations of soft sets and their properties. Furthermore, they[16] introduced fuzzy soft sets which combine the strength of both soft sets and fuzzy sets. As a generalization of the soft set theory, the fuzzy soft set theory makes description of the objective world more realistic, practical precise in some cases, making it very promising.

Since the notion of soft groups was proposed by Aktas and Cagman[2], then the soft set theory is used a new tool to discuss algebraic structures. Acar et.al[3] initiated the concepts of soft rings similar to soft groups. Liu et.al further the investigated isomorphism and fuzzy isomorphism theories of soft rings in [13], respectively. Soft sets were also applied to other algebraic structures such as near-rings[17], Γ-modulus and BCK/BCI-algebras[22].Bhakat and Das[6] proposed the concept of (α, β) -fuzzy subgroups.

Cagman et.al[7] studied on soft int-group, which are different from the definitions of soft groups[2]. The new approach is based on the inclusion relation and intersection of sets. It brings the soft set theory, the set theory, and the group theory together. On the basic of soft int-groups, Sezgin et.al[18] introduced the concept of soft intersection near-rings (soft int-near rings) by using intersection operation of sets and gave the applications of soft int near-rings to the near- ring theory. By introducing soft intersection, union products and soft characteristic functions, Sezer[19]made a new approach to the classical ring theory via the soft set theory, with the concepts of soft union rings, ideals and bi-ideal. Jun et.al[10] applied intersectional soft sets to BCK/BCI-algebras[11] an obtained many results. In the present paper , we provide the notion of (α, β) -fuzzy soft int-groups over fuzzy soft interior ideals and the notion of fuzzy coset , soft fuzzy quotient groups based on(-fuzzy soft int-ideals are established. Finally , isomorphism theorems of (α, β) – fuzzy soft int-groups related to invariant fuzzy soft sets are discussed.

2. PREMINARIES

In this section, we would like to recall some basic notions related to soft sets and soft int-groups. Throughout the paper, G denote arbitrary groups and e, e_1, e_2 and are the identity elements of G, G_1, and G_2 respectively. U is an initial universe and E is a set of parameters under the conditions with respect to U. A and B are subsets of E. The set of all subsets of U is denoted by P(U). Molodtsov[14] defined the concept of soft sets in the following way.

Definition 2.1: [15]A soft set f_A over U is defined as f_A: E→P(U) such that $f_A(x) = \emptyset$ if $x A \notin$

In other words, a soft set U is a parameterized family of subsets of the universe U. For all $\epsilon \in$ A, $f_A(\epsilon)$ may be considered as the set of ϵ-approximate elements of the soft set f_A. A soft set f_A over U can be presented by the set of ordered pairs: f_A = {($x, f_A(x)$) / $x \in$ E, $f_A(x)$= P (U)}……….(1). Clearly, a soft set is not a set. For illustration, Molodtsov consider several examples in (14).

If f_A is a soft set over U, then the image of f_A is defined by Im(f_A) = { $f_A(a)/a \in A$}. The set of all soft sets over U will be denoted by S(U). Some of the operations of soft sets are listed as follows.

Definition 2.2:[16]Let $f_A, f_B \in$ S(U). If $f_A(x) \subseteq f_B(x)$, for all $x \in$ E, then f_A is called a soft subset of f_B and denoted by $\subseteq f_B$. f_A and f_B are called soft equal, denoted by $f_A = f_B$ if and only if $f_A \subseteq f_B$ and $f_B \subseteq f_A$.

Definition 2.3: [18]Let $f_A, f_B \in$ S(U) and let χ be a function from A to B. Then the soft anti-image of f_A under χ denoted by $\chi(f_A)$, is a soft set over U definedby,

$$\chi_{f_A}(\mathrm{b}) = \begin{cases} \cap \{ f_A(a)/a \in A, \chi(a) = b\}, if\ \chi^{-1}(b) \neq \emptyset \\ 0 \qquad , \text{otherwise} \end{cases} \quad ……………(2)$$

for all $b \in$B. And the soft preimage of f_B underχ, denoted by $\chi^{-1}(f_B)$, is a soft set over U defined by $\chi^{-1}{}_{f_B}$(a) = $f_B(\chi(a))$, for all $a \in A$.

Note that the concept of level sets in the fuzzy set theory, Cagman et.al[7] initiated the concept of lower inclusions soft sets which serves as a bridge between soft sets and crisp sets.

Definition 2.4:[9] Let G be a group and $f_G \in$ S(U). Then f_G is called a soft intersection groupoid over U if $f_G(xy) \supseteq f_G(x) \cap f_G(y)$ for all $x, y \in G$. f_G is called a soft intersection group over U if the soft intersection groupoid satisfies $f_G(x^{-1}) = f_G(x)$ for all . $x \in G$

For the sake of brevity, soft intersection group is abbreviated by soft int-group throughout this paper.

Example: Assume that U=Z is the universal set and G=Z_b is the subset of parameters. We define a soft set f_G by $f_G(0)$ = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}

$f_G(1) = \{0, 2, 4, 6, 8, 10\}, f_G(2) = \{1, 3, 4, 6, 7\}, f_G(3) = \{0, 2, 3, 6, 9\}, f_G(4) = \{1, 3, 4, 6, 7\}$

$f_G(5) = \{0, 2, 4, 6, 8, 10\}$ .It is clear that $f_G(1 + z) \not\supseteq f_G(1) \cap f_G(z)$, implying f_G is not a soft int-group over U.

Definition 2.5:[23] Let U be a non-empty set. Then by a fuzzy set on U is meant a function A : U [0,1].A is called the membership function, A(x) is called the membership grade of x in A. We also write A= {(x, A(x)): x∈U}

Example: Consider U = { a, b, c ,d } and A : U [0,1] defined by A(a)=0, A(b)=0.7, A(c)=0.4, A(d)=1

Definition 2.6:[2] Let U be an initial universe, E be the set of all parameters and A ⊆ E. A pair (F, A) is called a fuzzy soft set over U where F: A → P (U) is a mapping from A into P (U) , where P (U) denotes the collection of all subsets of U.

Example: Consider the above example, here we cannot express with only two real numbers 0 and 1, we can characterized it by a membership function instead of crisp number 0 and 1, which associate with each element a real number in the interval [0,1].Then

$(f_A, E) = \{f_A(e_1) = \{(u_1, 0.7), (u_2, 0.5), (u_3, 0.4), (u_4, 0.2)\}, f_A(e_2) = \{(u_1, 0.5), (u_2, 0.1), (u_3, 0.5)\}$ is the fuzzy soft set .

Definition 2.7: Let f_G be a fuzzy soft set over U. f_G is called a (α, β)-fuzzy soft int-group of U if

(i) $f_G(xy) \cap \alpha \geq f_G(x) \cap f_G(y) \cup \beta$ (ii) $f_G(x^{-1}) \cap \alpha = f_G(x) \cup \beta$. For all $x, y \in G$.

Example:1 Let Z/(3) = { $\bar{0}, \bar{1}, \bar{2}$} be a modulo 3 residue class group, A={λ_1, λ_2}. Define a fuzzy soft set (F,A) over < Z/(3) , + > as ; F(λ_1)($\bar{0}$)=0.3, F(λ_1)($\bar{1}$)=0.6, F(λ_1)($\bar{2}$)=0.8, F(λ_2)($\bar{0}$)=0.4, F(λ_2)($\bar{1}$)=0.5, F(λ_2)($\bar{2}$)=0.7. It is easy verify that F(λ_1), F(λ_2) are fuzzy subgroups of < Z/(3) , + >. Therefore (F,A) is a fuzzy soft int-groups over < Z/(3) , + >.

Example:2 Let G= {e ,x ,y, z} be the group with the binary operation defined below.

*	e	x	y	z
e	e	x	y	z
x	x	z	e	y
y	y	e	z	x
z	z	y	x	e

Let A = {h_1, h_2} be the set of parameters. For each parameter h_1 ∈A, F(h_1): G →[0,1]. For each parameter we define

F(h_1) = *{ < e,0.6>, <x,0.75>, <y,0.62>, <z,0.31>}*

F(h_2) = *{ < e,0.77>, <x,0.88>, <y,0.92>, <z,0.7>}.*

Here (F,A) is fuzzy soft int-group.

Lemma 1: Let f_G be a fuzzy soft set over U. If f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group of G, then (i) $(f_G(x^{-1}) \cap \alpha) \cup \beta \geq (f_G(x) \cap \alpha) \cup \beta$.(ii) $f_G(x^{-1}) \cap \alpha \geq f_G(x) \cup \beta$ for all$x \in G$.

Proof:(i) Assume that f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group of G.

Then for all$x \in \boldsymbol{G}$, we get that

$$(f_G(x^{-1}) \cap \alpha) \cup \beta = (f_G(x^{-1}) \cap \alpha \cap \alpha) \cup \beta \geq ((f_G((x^{-1})^{-1}) \cup \beta) \cap \alpha) \cup \beta$$

$$= (f_G(x) \cap \alpha) \cup \beta.$$

(ii)It is straight forward.

Lemma2: Let f_G be a fuzzy soft set over U. If f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group of G, then

(i) $(f_G(e) \cap \alpha) \cup \beta \geq (f_G(x) \cap \alpha) \cup \beta$.(ii) $f_G(e) \cap \lambda \geq f_G(x) \cup \beta$ for all$x \in G$.

Proof: (i) Assume that f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group of G.

Then for all$x \in \boldsymbol{G}$, we get that

$$(f_G(e) \cap \alpha) \cup \beta = (f_G(xx^{-1}) \cap \alpha \cap \alpha) \cup \beta \geq ((f_G(x) \cap f_G(x^{-1})) \cup \beta) \cap \alpha) \cup \beta$$

$$= ((f_G(x) \cap \alpha) \cup \beta) \cap ((f_G(x^{-1}) \cap \alpha) \cup \beta) \geq (f_G(x) \cap \alpha) \cup \beta. \text{ (By Lemma:1)}$$

(ii)It is straight forward.

Combining lemma:2 and Definition:2.7, we obtain the following characterization of (α,β))-fuzzy soft int-groups.

Theorem 2.1:A fuzzy soft set f_G over U is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group over U if and only if

$f_G(xy^{-1}) \cap \alpha \geq f_G(x) \cap f_G(y) \cup \beta$ for all$\boldsymbol{x}, y \in G$.

Proof: Suppose that f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group over U. Then

$f_G(xy^{-1}) \cap \alpha \geq f_G(x) \cap f_G(y^{-1}) \cup \beta = f_G(x) \cap f_G(y) \cup \beta$ for all$\boldsymbol{x}, y \in G$.

Conversely, suppose that $f_G(xy^{-1}) \cap \alpha \geq f_G(x) \cap f_G(y) \cup \beta$ for all$\boldsymbol{x}, y \in G$.

First, choosing x=e yields $f_G(y^{-1}) \cap \alpha \geq f_G(y) \cup \beta$. Thus,

$f_G(y) \cap \alpha = f_G((y^{-1})^{-1}) \cap \alpha \geq f_G(y^{-1}) \cup \beta$. Hence $f_G(y) \cap \alpha = f_G(y^{-1}) \cup \beta$. Secondly

$f_G(xy) \cap \alpha = f_G(x(y^{-1})^{-1}) \cap \alpha \geq f_G(x) \cap f_G(y^{-1}) \cup \beta = f_G(x) \cap f_G(y) \cup \beta$. Therefore

f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group over U.

Theorem2.2: Let f_G over U is a (α,β)-fuzzy soft int-group over U and $x \in G$. Then

$f_G(xy) \cap \alpha \ \geq f_G(y) \cup \beta$ for all $y \in G$ if and only if $f_G(x) \cap \alpha = f_G(e) \cup \beta$.

Proof: Let $f_G(xy) \cap \alpha \ \geq f_G(y) \cup \beta$ for all $y \in G$.

Choosing $y = e$ yields $f_G(x) \cap \alpha \ \geq f_G(e) \cup \beta$, thus by lemma-2, $f_G(x) \cap \alpha = f_G(e) \cup \beta$.

Conversely, let $f_G(x) \cap \alpha = f_G(e) \cup \beta$. Then

$f_G(xy) \cap \alpha \ \geq f_G(x) \cap f_G(y) \cup \beta = f_G(e) \cap f_G(y) \cup \beta = f_G(y) \cup \beta$.

Theorem2.3: Let f_G and f_H be (α,β)-fuzzy soft int-group over U. Then $f_G \cap f_H$ is also a (α,β)-fuzzy soft int-group over U.

Proof: Let $(x_1,y_1), (x_2,y_2) \in$ G × H. Then

$f_{GH}\ ((x_1,y_1)(x_2,y_2)^{-1}) \cap\alpha = f_{GH}\ (x_1x_2^{-1},y_1y_2^{-1}) \cup \beta = f_G\ (x_1x_2^{-1}) \cap\ f_H(y_1y_2^{-1}) \cup \beta$

$\geq (f_G(x_1) \cap f_G(x_2) \cup \beta\ ) \ \cap \ (\ f_H(y_1) \cap f_H(y_2) \cup \beta\ ) = \ (f_G(x_1) \cap f_H(y_1) \cup \beta\ ) \ \cap \ (\ f_G(x_2) \cap f_H(y_2) \cup \beta) = f_{GH}\ (x_1,y_1) \cap f_{GH}\ (x_2,y_2) \cup \beta$.Therefore, $f_G \wedge f_H$ is a (α,β)-fuzzy soft int-group over U.

Note that $f_G \cup f_H$ is not a (α,β)-fuzzy soft int-group over U.

Definition 2.8:[22] Let $f_A, f_B \in$ S (U). Then, ∩-Product and V- Sum of f_A and f_B, denoted by $f_A f_B$ and $f_A \vee f_B$, are defined by $f_{AB}(x,y) = f_A(x) \cap f_B(y)$, $f_{A\vee B}(x,y) = f_A(x) \cup f_B(y)$ for all x ,$y \in E$ respectively.

Definition 2.9: Let f_G and f_H be (α,β)-fuzzy soft int-groups over U. Then, the product of soft int-groups f_G and f_H is defined as $f_G \times f_H = f_{G\times H}$ where

$f_{G\times H}(x,y) \cap \alpha = f_G(x) \times f_H(y) \cup \ \beta$ for all $(x,y) \in$ G × H.

Theorem2.4: If f_G and f_H be (α,β)-fuzzy soft int-groups over U, then so is $f_G \times f_H$ over U×U.

Proof: By definition:2.9, let $f_G \times f_H = f_{G\times H}$ where

$f_{G\times H}(x,y) \cap \alpha = f_G(x) \times f_H(y) \cup \ \beta$ for all $(x,y) \in$ G × H.

Then for all $(x_1,y_1), (x_2,y_2) \in$ G × H,

$f_{G\times H}\ ((x_1,y_1)(x_2,y_2)^{-1}) \cap \alpha = f_{G\times H}\ (x_1x_2^{-1},y_1y_2^{-1}) \cap \alpha = f_G\ (x_1x_2^{-1}) \times\ f_H(y_1y_2^{-1}) \cup \beta$

$\geq (f_G(x_1) \cap f_G(x_2) \cup \beta\ ) \ \times \ (\ f_H(y_1) \cap f_H(y_2) \cup \beta\ ) = \ (f_G(x_1) \times f_H(y_1) \cup \beta\ ) \ \cap \ (\ f_G(x_2) \times f_H(y_2) \cup \beta) = f_{G\times H}\ (x_1,y_1) \cap f_{G\times H}\ (x_2,y_2) \cup \beta$.

Hence, $f_G \times f_H = f_{G\times H}$ is fuzzy soft int-groups over U×U.

Theorem2.5: Let f_H be $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group over U and h be a homomorphism from G to H. Then $h^{-1}(f_H)$ is $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group over U.

Proof: Let x, $y \in$ G. Then,

$$\boldsymbol{h}^{-1}(f_H)(xy) \cap \alpha = f_H(h(xy)) \cap \alpha = f_H\big(h(x)h(y)\big) \cap \alpha \ \geq f_H(h(x)) \cap \ f_H(h(y)) \cup \beta$$

$$= \boldsymbol{h}^{-1}(f_H)(x) \cap h^{-1}(f_H)(y) \ \cup \beta.$$

Also,

$$h^{-1}(f_H)(x^{-1}) \cap \alpha = f_H(\boldsymbol{h(x^{-1})}) \cap \ \alpha \ = f_H((h(x))^{-1}) \cap \alpha = f_H\big(h(x)\big) \cup \beta = \boldsymbol{h}^{-1}(f_H)(x) \cup \beta$$

Hence, $h^{-1}(f_H)$ is $(\boldsymbol{\alpha},\beta)$-fuzzy soft int-group over U.

Definition 2.8: A fuzzy soft set f_G over U is called $(\boldsymbol{\alpha},\beta)$-fuzzy soft interior ideal of G if it satisfies $f_G(xy) \cap \alpha \ \geq f_G(x) \cap f_G(y) \cup \beta$, $f_G(xwy) \cap \alpha \geq f_G(x) \cup \beta$ for all $x, y, w \in$ G.

Example: Let S= {0, e,f,a,b} be a set with the following cayley table.

.	0	e	f	a	b
0	0	0	0	0	0
e	0	e	0	a	0
f	0	0	f	0	b
a	0	a	0	0	e
b	0	0	b	f	0

Let h : G→ [0,1] be a fuzzy soft set in G defined by h(0) = h(e) =h(f) = 1, h(a) = h(b) = 0.
By routine calculations one show that h is an $(\boldsymbol{\alpha},\beta)$-fuzzy soft interior ideals.

Definition 2.9: Let f_G be a $(\boldsymbol{\alpha},\beta)$-fuzzy soft interior ideal of G. Then E Im(f_G) is called the extended image set of f_G, where E Im(f_G) = Im(f_G) $\cup$ (α,β).

Now we characterize $(\boldsymbol{\alpha},\beta)$-fuzzy soft interior ideals by upper inclusion.

Theorem 2.6: Let f_G be a fuzzy soft set over U and E Im(f_G) a totally order set in inclusion. Then f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft interior ideal of G if and only if $\cup(f_G{:}\lambda)$ is an ideal of G, whenever it is non empty, for each λ ⊆ U where $\beta \leq \lambda < \alpha$.

Proof: Assume that f_G is a (α,β)-fuzzy soft interior ideal of G and ( ) is $\cup(f_G{:}\lambda)$ non empty.

It is sufficient to show that $x\ y \in \cup(f_G{:}\lambda)$. Let $x,y \in \cup(f_G{:}\lambda)$ it follows that $f_G(x) \geq \lambda$ and $f_G(y) \geq \lambda$. Since f_G is a $(\boldsymbol{\alpha},\beta)$-fuzzy soft interior ideal of G and E Im(f_G) a totally order set, then

$f_G(xy) \cap \alpha \quad \geq f_G(x) \cap f_G(y) \cup \beta \geq \lambda \cup \lambda \cup \lambda = \lambda < \boldsymbol{\alpha}$,

$f_G(xwy) \cap \alpha \geq f_G(x) \cup \beta \geq \lambda \cup \lambda = \lambda < \boldsymbol{\alpha}$.

And thus $f_G(xy) \geq \alpha$. Hence $x\,y \in \cup(f_G{:}\,\lambda)$. Therefore $\cup(f_G{:}\,\lambda)$ is an ideal of G.

Conversely, assume that $\cup(f_G{:}\,\lambda)$ is an ideal of G, whenever it is non empty, for each $\lambda \subseteq$ U where $\beta \ \leq \lambda \ < \alpha$ Suppose that $f_G(xy) \cap \alpha \geq f_G(x) \cap f_G(y) \cup \beta$ does not holds for some x, $y \in$ G; then there exists $x_0, y_0 \in$G such that $f_G(x_0y_0) \cap \alpha \leq \lambda = (f_G(x_0) \cap f_G(y_0) \cup \beta)$. There fore $f_G(x_0) \cap f_G(y_0) \supseteq \lambda$; that is $x_0y_0 \notin \cup(f_G{:}\,\lambda)$ which is contradiction. Hence $f_G(xy) \cap \alpha \quad \geq f_G(x) \cap f_G(y) \cup \beta$, for all x, $y \in$ R. Similarly, we can prove that $f_G(xwy) \cap \alpha \geq f_G(x) \cup \beta$ for all x, $y, w \ \in$ G. Thus, f_G is a $(\boldsymbol{\alpha}, \beta)$-fuzzy soft interior ideal of G.

Theorem2.7: Let f_G be a fuzzy soft set over U and χ is a group homomorphism from G_1 tG_2. If $f_{G_1}$is a (α)βfuzzy soft interior ideal of G_2, then $\chi^{-1}(f_{G_2})$ is a $(\boldsymbol{\alpha}, \beta$-fuzzy soft interior ideal of G_1.

Proof: Let $x_1, x_2 \in G_1$. Then$\chi \quad ^{-1}(f_{G_2})(x_1x_2) \cap \alpha = \quad f_{G_2}(\chi(x_1).\chi(x_2)) \cap \alpha$

$\geq f_{G_2}(\chi(x_1x_2)) \cap \alpha = f_{G_2}(\chi(x_1)) \cap f_{G_2}(\chi(x_2)) \quad \beta \chi =$

$^{-1}(f_{G_2})(x_1) \cap \quad ^{-1}(f_{G_2})(x_2) \cup \beta$

Moreover, we have

$$\chi^{-1}(f_{G_2})(x_1wx_2) \cap \alpha = f_{G_2}(\chi(x_1wx_2)) \cap \alpha \ = f_{G_2}(\chi(x_1).\chi(w).\chi(x_2)) \cap \alpha$$

$$\geq (f_{G_2}(\chi(x_1))) \cup \beta \ = \chi^{-1}(f_{G_2})(x_1) \ \cup \beta$$

Hence $\chi^{-1}(f_{G_2})$ is a $(\boldsymbol{\alpha}, \beta)$-fuzzy soft interior ideal of G_1.

Theorem 2.8: Let f_{G_1} be a fuzzy soft set over U and χ a group epimorphism from G_1 to G_2.If $f_{G_1}$is a $(\boldsymbol{\alpha}, \beta)$-fuzzy soft interior ideal of G_1, then $\chi(f_{G_1})$ is $(\boldsymbol{\alpha}, \beta)$-fuzzy soft interior ideal of G_2 and $(\chi(f_{G_1})(e_2) \cap \alpha) \cup \beta = (\ f_{G_1})(e_1) \cap \alpha) \cup \beta$.

Proof: Let $y_1, y_2 \in G_2$ and $f_{G_1}$is a $(\boldsymbol{\alpha}, \beta)$-fuzzy soft interior ideal of G_1. Since χ is a group epimorphism from G_1 to G_2, then $\chi^{-1}(y_1) \neq \emptyset$ and $\chi^{-1}(y_2) \neq \emptyset$. And thus, there exist $x_1, x_2 \in G_1$ such that $\chi(x_1) = y_1, \chi(x_2) = y_2$. There fore , we have

$\chi(f_{G_1})(y_1y_2) \cap \alpha = \cap \{f_{G_1}(x_1x_2) / \chi(x_1x_2) = y_1y_2\} \cap \alpha = \cap \{f_{G_1}(x_1x_2) \cap \alpha / \chi(x_1x_2) = y_1y_2\}$

$\geq \cap \{f_{G_1}(x_1) \cap f_{G_1}(x_2) \cup \beta / \chi(x_1) = y_1, \chi(x_2) = y_2\} \ = \cap \{f_{G_1}(x_1) / \chi(x_1) = y_1\} \cap \{f_{G_1}(x_2) / \chi(x_2) = y_2\} \cup \beta = \chi(f_{G_1})(y_1) \cap \chi(f_{G_1})(y_2) \cup \beta$

$\chi(f_{G_1})(y_1wy_2) \cap \alpha = \cap \{f_{G_1}(y_1wy_2) / \chi(x_1wx_2) = y_1wy_2\} \cap \alpha$

$= \cap \{f_{G_1}(y_1wy_2) \cap \alpha / \chi(x_1wx_2) = y_1wy_2\}$

$$\geq \cap \{f_{G_1}(\; y_1) \cap \alpha / \chi(x_1) = y_1\} = \cap \{ f_{G_1}(x_1)/ \chi(x_1) = y_1\} \cup \beta \;\; = \chi(f_{G_1})(y_1) \cup \beta$$

Therefore $\chi(f_{G_1})$ is (α,β)-fuzzy soft interior ideal of G_2.

By lemma-2, we have

$$(\chi(f_{G_1})(e_2) \cap \alpha) \cup \beta = (\cap \{f_{G_1}(x)/x \in G_1, \chi(x) = e_2\} \cap \alpha) \cup \beta$$

$$= \cap \{(f_{G_1}(x) \cap \alpha) \cup \beta / x \in G_1, \chi(x) = e_2\} = (f_{G_1}(e_1) \cap \alpha) \cup \beta.$$

3. SOFT FUZZY QUOTIENT GROUPS

The main purpose of this section is to give an approach for constructing soft fuzzy quotient groups based on (α, β))-fuzzy soft interior ideals. Such approaches involve the concept of soft fuzzy cosets. In addition, some simple characterizations of soft fuzzy cosets are presented.

Definition 3.1: Let f_G be a (α,β)-fuzzy soft int-group of G over U and $g \in G$. Then, a soft fuzzy coset $g \oplus f_G$ of f_G is defined by $(g\oplus f_G)(x) = (f_G(x-g) \cap \alpha) \cup \beta$, for all $x \in G$.

Main results

Theorem3.1: Let f_G be a (α,β)-fuzzy soft int-group of G over U and $a, b \in G$.Then

$(f_G(ab) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$ if and only if $(f_G(ba) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$.

Proof: Suppose that $(f_G(ba) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$.Since f_G is (α,β)-fuzzy soft int-group, then $(f_G(ab) \cap \alpha) \cup \beta = (f_G(ab) \cap \alpha \cap \alpha) \cup \beta \;\; \geq ((f_G(ba) \cup \beta) \cap \alpha) \cup \beta$

$$= (f_G(ba) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$$

By lemma-2, we have,

$(f_G(e) \cap \alpha) \cup \beta \;\; \geq (f_G(ab) \cap \alpha) \cup \beta$.Thus, $(f_G(ab) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$.

Conversely, assume that $(f_G(ab) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$. We can prove that $(f_G(ba) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$ in a similar way.

Proposition3.1: Let f_G be a (α,β)-fuzzy soft int-group of G over U and $a, b \in G$.Then $a \oplus f_G = b \oplus f_G$ if and only if $(f_G(ab) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$.

Proof: Suppose that $(f_G(ab) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$.

Then $(b\oplus f_G)(x) = (f_G(xb) \cap \alpha) \cup \beta \;\; = (f_G(xaa^{-1}b) \cap \alpha) \cup \beta$

$$= (f_G(xaa^{-1}b) \cap \alpha \cap \alpha) \cup \beta \;\; \geq ((f_G(xa) \cap f_G(a^{-1}b) \;\cup \beta) \;\cap \alpha) \cup \beta$$

$$= \; ((f_G(xa) \cap \alpha) \cup \beta) \cap ((f_G(a^{-1}b) \cap \alpha) \cup \beta) = \; ((f_G(xa) \cap \alpha) \cup \beta) \cap ((f_G(e) \cap \; \alpha) \cup \beta)$$

$$\geq (f_G(xa) \cap \alpha) \cup \beta = (a \oplus f_G)(x) \text{ for all } x \in G.$$

Therefore $b \oplus f_G \geq a \oplus f_G$. Similarly we can show that $a \oplus f_G \geq b \oplus f_G$. Hence $b \oplus f_G = a \oplus f_G$

Conversely, assume that $a \oplus f_G = b \oplus f_G$.

It follows that $(f_G(ab) \cap \alpha) \cup \beta = (b \oplus f_G)(a) = (a \oplus f_G)(a) = (f_G(e) \cap \alpha) \cup \beta$.

Based on the above proposition, we give a property related to soft fuzzy cosets as follows.

Proposition3.2: Let f_G be a $(\boldsymbol{\alpha}, \beta)$- fuzzy soft interior ideal over U and $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, y \in G$. If $x \oplus f_G = a \oplus f_G$, $y \oplus f_G = b \oplus f_G$, then $xy \oplus f_G = ab \oplus f_G$, $xwy \oplus f_G = a \oplus f_G$.

Proof: Suppose $x \oplus f_G = a \oplus f_G$.$y \oplus f_G = b \oplus f_G$.

Then, $(f_G(xa) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$ and $(f_G(yb) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$, by proposition 3.1.Since f_G is a $(\boldsymbol{\alpha}, \beta)$-fuzzy soft interior ideal, then

$$(f_G((xyab)) \cap \alpha) \cup \beta = (f_G((xa.\,yb)) \cap \alpha) \cup \beta = (f_G((xa.\,yb)) \cap \alpha \cap \alpha) \cup \beta$$

$$\geq ((f_G(xa) \cap f_G(yb) \cup \beta) \cap \alpha) \cup \beta$$

$$= (f_G(xa) \cap \alpha) \cap (f_G(yb) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$$

On the other hand, it follows from lemma:2 that $(f_G(e) \cap \alpha) \cup \beta \geq (f_G((xyab)) \cap \alpha) \cup \beta$.

Hence $(f_G((xyab)) \cap \alpha) \cup \beta = (f_G(e) \cap \alpha) \cup \beta$, and so $xy \oplus f_G = ab \oplus f_G$.

More over $(f_G((xwyab)) \cap \alpha) \cup \beta = (f_G(xawy.\,aywb) \cap \alpha \cap \alpha) \cup \beta$

$$= (f_G(xay) \cap \alpha) \cup \beta = (f_G(xay) \cap \alpha \cap \alpha) \cup \beta$$

$$\geq ((f_G(xa) \cup \beta) \cap \alpha) = (f_G(xa) \cap \alpha) \cup \beta$$

$$= (f_G(e) \cap \alpha) \cup \beta.$$

According to lemma-2, we get that $(f_G(e) \cap \alpha) \cup \beta \geq (f_G((xyab)) \cap \alpha) \cup \beta$.

Therefore, $(f_G(e) \cap \alpha) \cup \beta \geq (f_G((xyab)) \cap \alpha) \cup \beta$; that is $xy \oplus f_G = ab \oplus f_G$.

In view of proposition 3.2, we have the following result.

Proposition3.3: Let f_G be a $(\boldsymbol{\alpha}, \beta)$- fuzzy soft interior ideal over U.Then $(G/f_G, .)$ is a group, where $G/f_G \triangleq \{ a \oplus f_G / a \in G\}$, $(x \oplus f_G)\,(y \oplus f_G) \triangleq xy \oplus f_G$, and $(x \oplus f_G) w\, (y \oplus f_G) \triangleq xy \oplus f_G$, for all $\boldsymbol{x}, y \in G$.

Proof: It is straight forward.

Definition 3.2: Let f_G be a (α,β)- fuzzy soft interior ideal over U. Then $(G/f_G,.)$is called a soft fuzzy quotient group.

Theorem3.2: Let f_G be a (α,β)- fuzzy soft interior ideal over U. Then $G/f_G^* \cong G/f_G$.

Proof: Assume that h: $G \rightarrow G/f_G$ such that $h(x) = x \oplus f_G$, for all $\in G$. It is easy to see that h is a surjective homomorphism from G to G/f_G.

Since Kerl(h) = $\{ x \in G/h(x) = e \oplus f_G\} = \{ x \in G/x \oplus f_G = e \oplus f_G\} = \{ x \in G/(f_G(x) \cap \alpha) \cup \beta$ $= (f_G(e) \cap \alpha) \cup \beta\} = f_G^*$.Therefore, $G/f_G^* \cong G/f_G$.

Definition 3.3: Let $\chi : G_1 \rightarrow G_2$ be a group homomorphism. A fuzzy soft set of f_{G_1} over U is called invariant fuzzy soft set with respect to χ if $\chi(x_1) = \chi(x_2)$ implies $f_{G_1}(x_1) = f_{G_1}(x_2)$ for all $x_1, x_2 \in G_1$.

Proposition 3.4: Let $\chi : G_1 \rightarrow G_2$ be a group homomorphism and f_{G_2} a fuzzy soft set of G_2 over U. Then, $\chi^{-1}(f_{G_2})$ is an invariant fuzzy soft set with respect to χ.

Proof: Let $x_1, x_2 \in G_1$ such that $\chi(x_1) = \chi(x_2)$. Then $\chi^{-1}(f_{G_2})(x_1) = f_{G_2}(\chi(x_1)) = f_{G_2}(\chi(x_2))$ $= \chi^{-1}(f_{G_2})(x_2)$.Hence, $\chi^{-1}(f_{G_2})$ is an invariant fuzzy soft set with respect to χ.

Next, we establish isomorphism theorem on (α,β)-fuzzy soft int-groups.

Theorem3.3: [Isomorphism theorem]Let $\chi : G_1 \rightarrow G_2$ be an epimorphism and let (α,β)-fuzzy soft interior ideal f_{G_1}be a invariant fuzzy soft set with respect to χ. Then $G_1/f_{G_1} \cong G_2/\chi(f_{G_1})$.

Proof: Let $\chi : G_1 \rightarrow G_2/\chi(f_{G_1})$ be a mapping such that $\chi(x) = \chi(x) \oplus f_{G_1}$, for all $x \in G_1$. Obviously, χ is an epimorphism. Since f_{G_1}be a invariant fuzzy soft set with respect to χ,

$\text{Ker}(\chi) = \{x \in G_1 / \chi(x) = e_2 \oplus \chi(f_{G_1})\} = \{x \in G_1 / \chi(x) \oplus \chi(f_{G_1}) = e_2 \oplus \chi(f_{G_1})\}$

$= \{x \in G_1 / \chi(f_{G_1})(\chi(x) \cap \alpha) \cup \beta\} = \{\chi(f_{G_1})(e_2) \cap \alpha) \cup \beta\} = \{x \in G_1 / x \oplus f_{G_1} = e_1 \oplus f_{G_1}\} =$ $f_{G_1}^*$ Therefore, $G_1/f_{G_1}^* \cong G_2/\chi(f_{G_1})$. By theorem 3.2 we have $G_1/f_{G_1}^* \cong G_1/f_{G_1}$. Hence $G_1/f_{G_1} \cong G_2/\chi(f_{G_1})$.

Proposition3.5: Let $\chi : G_1 \rightarrow G_2$ be an epimorphism and let (α,β)-fuzzy soft interior ideal f_{G_2}be a invariant fuzzy soft set with respect to χ. Then $G_1/\chi^{-1}(f_{G_2}) \cong G_2/f_{G_2}$.

Proof: It follows from the theorem 3.2 and proposition 3.4 that $\chi^{-1}(f_{G_2})$ is a α,β- fuzzy soft interior ideal of G_1 and $\chi^{-1}(f_{G_2})$ is a invariant fuzzy soft set with respect to χ. Since χ is an epimorphism, then $\chi(\chi^{-1}(f_{G_1})) = f_{G_2}$. By theorem3.3, we get $G_1/\chi^{-1}(f_{G_2}) \cong G_2/f_{G_2}$.

Conclusion: In this paper, using fuzzy soft sets and intersection of sets, we have defined (α,β)- fuzzy soft int-group that is new type of fuzzy soft group on a fuzzy soft set and then make theoretical studies of (α,β)-fuzzy soft int-groups and (α,β)-fuzzy soft interior ideal in more detail and improved several results. We have focused on (α,β)-fuzzy soft int-groups and (α,β)- fuzzy soft interior ideal, anti-image of fuzzy soft set and investigate these notions with respect to fuzzy soft int-groups and fuzzy soft interior ideal .

Future work: To extend our work, further research can be done to study the properties of fuzzy soft int-group in other algebraic structures such as modules, rings and fields.

REFERENCE

[1].K. T. Atanassov, "Intuitionistic fuzzy sets," Fuzzy Sets and Systems, vol. 20, no. 1, pp. 87– 96, 1986.

[2].H. Aktaş and N. Çağ man, "Soft sets and soft groups," Information Sciences, vol. 177, no. 13, pp. 2726–2735, 2007.

[3].U. Acar, F. Koyuncu, and B. Tanay, "Soft sets and soft rings," Computers and Mathematics with Applications, vol. 59, no. 11, pp. 3458–3463, 2010.

[4].M. I. Ali, F. Feng, X. Liu, W. K. Min, and M. Shabir, "On some new operations in soft set theory," Computers and Mathematics with Applications, vol. 57, no. 9, pp. 1547–1553, 2009.

[5].G.L.Booth, A note on Γ -near-rings Stud. Sci. Math. Hung. 23(1988), 471-475.

[6].S. K. Bhakat and P. Das, "Fuzzy subrings and ideals redefined," Fuzzy Sets and Systems, vol. 81, no. 3, pp. 383–393, 1996.

[7].N. Çağman, F. Çıtak, and H. Aktas, "Soft int-group and its applications to group theory," Neural Computing & Applications, vol. 56, no. 5, pp. 1408–1413, 2008.

[8].F. Feng, Y. Li, and N. Çağman, "Soft subsets and soft product operations," Information Sciences, vol. 232, pp. 44–57, 2013.

[9].F. Feng, Y. Li, and N. Çağ man, "Generalized uni-int decision making schemes based on choice value soft sets," European Journal of Operational Research, vol. 220, no. 1, pp. 162–170, 2012.

[10].Y. B. Jun, "Soft BCK/BCI-algebras," Computers and Mathematics with Applications, vol. 56, no. 5, pp. 1408–1413, 2008.

[11].Y. B. Jun, K. J. Lee, and E. H. Roh, "Closed int soft BCI-ideals and int soft c-BCI-ideals," Journal of Applied Mathematics, vol. 2012, Article ID 125614, 15 pages, 2012.

[12].X. Liu, D. Xiang, J. Zhan, and K. P. Shum, "Isomorphism theorems for soft rings," Algebra Colloquium, vol. 19, no. 4, pp. 649–656, 2012.

[13].X. Liu, D. Xiang, and J. Zhan, "Fuzzy isomorphism theorems of soft rings," Neural Computing and Applications, vol. 21, no. 2, pp. 391–397, 2012.

[20]. Bh. Satyanarayana, Contributions to near-ring theory, Doctoral Thesis, Nagarjuna Univ.1984.

[21]. Yongwei Yang ,Xiaolong Xin and Pengfei He , " Applications of soft union sets in the ring theory" Journal of Applies Mathematics,volume 2013.

[22].M. Zhou, D. Xiang, and J. Zhan, "The characterization of Γ-modules in terms of fuzzy soft Γ-submodules," Applied Mathematics B, vol. 28, no. 2, pp. 217–239, 2013.

[23].L. A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, no. 3, pp. 338–353, 1965.

Hybrid Encryption Algorithm Based Improved RSA and Diffie-Hellman

Miss. Renushree Bodkhe* , Prof. Vimla Jethani*
* Ramrao Adik Institute of Technology,
Nerul, Navi Mumbai

ABSTRACT

Internet and Network applications have seen a tremendous growth in the last decade. As a result incidents of cyber attacks and compromised security are increasing. This requires more focus on strengthening and securing our communication. One way to achieve this is cryptography. Although a lot of work has been done in this area but this problem still has scope of improvement. In this paper we have focused on asymmetric key cryptography. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption. No other key can decrypt the message, not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. RSA is a well known public key cryptography algorithm. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. So to improve the security, this scheme presents a new cryptography algorithm based on novel method by combining the two most popular algorithms RSA as Improved RSA (IRSA) and Diffie-Hellman in order to achieve more security.

Keywords: IRSA, Cryptography, DH, Encryption, Decryption, etc.

1. INTRODUCTION

One of the most important techniques to secure communication in the presence of third party is cryptography. Cryptography is the science which uses mathematics to encrypt and decrypt data. This science enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. In asymmetric cryptography, the encryption and decryption keys are different on both the sides. Hybrid cryptography is a combination of both symmetric and asymmetric cryptographic techniques. Hybrid cryptography is very effective indeed in providing high degree of security because whatever the problems associated with symmetric-key cryptographic techniques were solved when asymmetric cryptographic mechanism is used. Encryption is one of the principal means to grantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc.

Encryption is the process of conversion of data (called plain text) into an unreadable form (called a cipher text), this cipher text cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so that it can be understood by the people who are authorized to read that data [3]. There exist many encryption algorithms that are widely used for information security. They can be categorized into symmetric (private) and asymmetric (public) key encryption. In practice, in order toachieve the optimal efficiency, the symmetric keyalgorithms and public key cryptography algorithms aregenerally combined together. Also Public-key cryptography can be used with secret-key cryptography to get the best of both worlds. Thus in this paper we have proposed a hybrid cryptographic algorithms by a combination of improved RSA and Diffie-Hellman. This combined approach is intended to get security advantage of public key system and speed advantage of secret key system.

1.1 Asymmetric Cryptography

In Asymmetric cryptography a pair of keys is used to encrypt and decrypt a message so that it is transmitted securely. Initially, a network user receives a public and private key pair from a Certificate Authority. The process of encryption using asymmetric cryptography can be explained by following steps -

- Use a key (public key) to encrypt a message.
- Another (private key) to decrypt a message.
- Private Key known to owner and used only by owner.

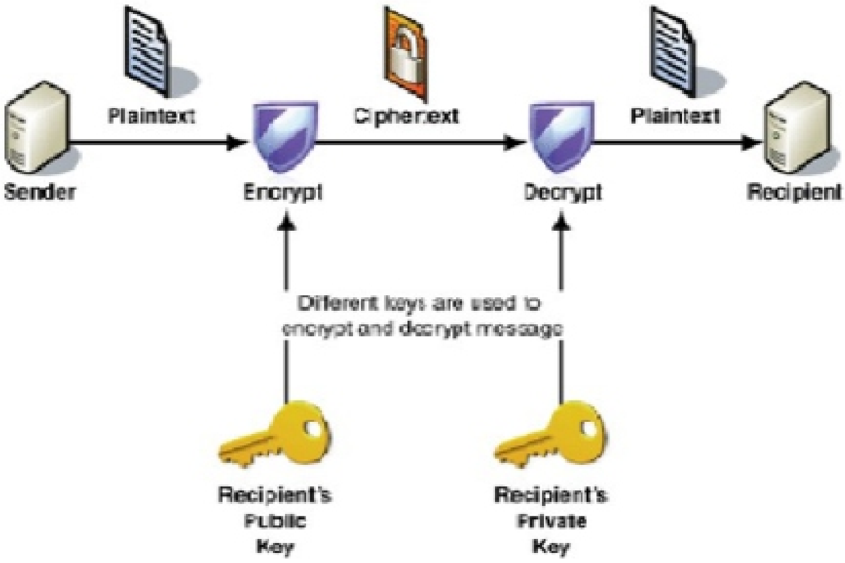


Figure 1: Asymmetric Key Encryption [7]

The advantage of using asymmetric key encryption is that it provides better key distribution and scalability in comparison of symmetric systems. RSA, Elliptic Curve Cryptosystem (ECC), Diffie-Hellman, El Gamal, Digital Signature Algorithm (DSA), Knapsack are some of the standard Asymmetric Key Algorithms.

1.2 RSA Algorithm

At present, the best known and most widely used public key system is RSA. A combined encryption algorithm is proposed in this thesis. That is, the algorithm security is greatly improved. The combined encryption algorithm is completely validated, and its security is very high.

Steps of Algorithm for Key Generation:

1. Choose two distinct prime numbers P and Q.
2. Calculate N = P x Q. (n is used as mod for both the public and private keys).
3. Select the public key (i.e. encryption key) E such that it is not a factor of (P – 1) and (Q - 1).

4. Select the private key (i.e. the decryption key) Dsuch that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1.
5. For encryption, calculate the cipher text Cfrom the plain text PT as follows: CT = PTEmod N.
6. Then send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT fromthe cipher text CT as follows: PT = CTD mod N.

1.3 Diffie-Hellman Algorithm

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure Connectivity protocols on the Internet. Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. This shared secret is important between two users who may not have ever communicated previously, so that they can encrypt their communications. Steps of this Algorithm are as:

1. Taking two numbers "P" and "G" "P" is a largeprime number "G" is called the base.
2. Picks a secret number "A" as first secretnumber = A, then picks another secret number"B" as second secret number = B.
3. Computes first public number X = GA mod P,and public number = X. Then computes secondpublic number Y = GB mod P, and publicnumber = Y.
4. Exchange their public numbers.
5. First knows P, G, A, X, Y, Second knows P, G,B, X, Y.
6. Computes First session key as KA = YA mod P OR KA = (GB mod P) A mod P OR KA = (GB)A mod P OR KA = GBA mod P.
7. Computes second session key as KB = XB modP OR KB = (GA mod P) B mod P OR KB =(GA) B mod P OR KB = GAB mod P.
8. Fortunately for Both by the laws of algebra,First session key "KA" is the same as Secondsession key "KB", or KA = KB = K.
9. Now, we have both the secret value as "K".

2. LITERATURE SURVEY

This section gives the detail of topic survey and review the work done by different authors in this field.

2.1 Overview

Yi Chen, Hong Chen, Hongqian, Chen, Xianchen Cheng [1] they first analyzed the characteristics of data and security problems in DIS network. For the real-time interactive data in DIS network, a stream cipher algorithm based on Logistic chaotic map (Logistic-EA) was presented. In this algorithm, the key stream was generated by Logistic chaotic map. The cipher text was gotten by executing XOR operation of plaintext and key stream. Logistic-EA has high security level and high encryption speed. For the non-real-time data, a hybrid encryption algorithm based on the chaos theory and AES (Chaos-AES) was presented. In this algorithm, the initial key and round key were generated by logistic chaotic map. Chaos-AES increased key space and implemented one-time pad. So that the cipher text encrypted by this algorithm is harder to break. The experiment results indicate that the algorithms above are effective in the DIS network.

Subhasis Mukherjee, MaynulHasan, Bilal Chowdhury, Morshed Chowdhury [2] the use of RFID (Radio Frequency Identification) technology can be employed for tracking and detecting each container, pallet, case, and product uniquely in the supply chain. It connects the supply chain stakeholders (i.e., suppliers, manufacturers, wholesalers/distributors, retailers and customers) and allows them to exchange data and product information. Despite these potential benefits, security issues are the key factor in the deployment. So they proposes a hybrid approach to secure RFID transmission in Supply Chain Management (SCM) systems using modified Wired Equivalent Encryption (WEP) and Rivest, Shamir and Adleman (RSA) cryptosystem.Their proposed system also addresses the common loop hole of WEP key algorithm and makes it more secure compare to the existing modified WEP key process Kirtiraj B Hatele, Prof. AmitSinhal ,Prof. Mayank P Athak [3] They proposed hybrid security protocol architecture offeredhigh degree of security especially against square attacksand efficient in terms of time. The given plain text can be encrypted with the help of AES (Advance encryptionstandard) and the derived cipher text can be communicatedto the destination through any secured channel.Simultaneously the Hash value is calculated through MD5for the same plain text, which already has been convertedinto the cipher text by AES. This Hash value has beenencrypted with Dual RSA and the encrypted message ofthis Hash value also sent to destination.Now at the receiving end, hash value ofDecrypted plaintext is calculated with MD5 and then it iscompared with the hash value of original plaintext which iscalculated at the sending end for its integrity. By this it is able to know whether the original text being altered ornot during transmission in the communication medium. The intruders may try to hack the original information fromthe encrypted messages. Although intuder he may be able to trapboth the encrypted messages of plain text and the hashvalue but he will not be able to decrypt these messages toget original one. Hence the message can be communicated to the destination in a highly secured manner.

Lili Yu, Weifeng Wang Zhijuan Wang [4] the combined encryption algorithm is successfully made by using the initial encryption algorithm, Micro Genardencryption algorithm and the famous Base64 encryption algorithm. That is, in accordance with the order of the initialencryption algorithm, the improved Micro Genard encryption algorithm and the famous Base64 encryption algorithm, theuser‟s information is gradually encrypted, and the algorithm security is greatly enhanced. Besides, to video surveillance software system for instance, which is widely used in the field of the traffic security management, the combined encryption algorithm is completely validated, and its security is very high.
Smita P. BansodVanita M. Mane Leena R. Ragha [5] this paper is based on hybrid cryptographic techniques based on DES and RSA algorithms to achieve data encryption and compression technique to store large amount of data. A combination of both provides superior security control. The suggested algorithm is modified BPCS (Bit Plane Complexity Segmentation) steganography technique that can replace all the “noise-like” regions in all the bit-planes of the cover image with secret data without deteriorating the image quality. According to the experiments, the messages can be successfully camouflaged in the cover image, and the stego images have satisfactory quality. Moreover, our scheme allows for a large capacity of embedded secret data and can be extracted from stego-image without the assistance of original image.

Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan [6] proposes a hybrid crypto system that utilizes benefits of both symmetric key and public key cryptographic methods. Symmetric key algorithms (DES and AES) are used in the crypto system to perform data encryption. Public key algorithm (RSA) is used in the cryptosystem to provide key encryption before key exchange. Combining both the symmetric-key and public-key algorithms provides greater security and some unique features which are only possible in this hybrid system. The cryptosystem design is modelled using Verilog HDL. The implementation has various modules for DES, AES and RSA. The implementation also has a pseudorandom number generation unit for random generation of keys and a GCD computation unit for RSA. All the hardware modules are designed by Register Transfer Level (RTL) modelling of Verilog HDL using ModelSimSE 5.7e.

3. HYBRID ENCRYPTION

3.1 Limitations of RSA

- If any one of p, q, e, d is known, then the other values can be calculated. So secrecy is important.
- It is important to make sure that message lengthShould be less then bit length otherwise the algorithm will fail.
- Due to the usage of public key RSA is much slower than any other symmetric cryptosystems.
- The length of plain text that can be encrypted islimited to the size of n=p*q.

Each time RSA initialization process requires the random selection of two very large prime numbers (p and q).

3.2 Limitations of Diffie Hellmen

- It is easily susceptible to man-in-the-middle attacks.
- The algorithm cannot be used to encrypt messages.
- There is also a lack of authentication.
- The computational nature of the algorithm couldbe used in a denial-of-service attack very easily.

3.3 Hybrid Encryption Algorithm on RSA and Diffie-Hellmen Steps of this algorithm are as:-

1. Choose two large prime numbers P and Q.

a. Calculate N = P x Q.
b. Select public key (i.e encryption key) E such that it is not a factor of (P – 1) and (Q -1).
c. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1
d. Suppose R, S and G is automatic generated prime constants.
e. And put the value of E and D from above as secretnumber such that A=E and B=D.

2. Now calculate following as public number X= GA mod R

Y= GB mod R

3. Calculate session key with formula

KA = YA mod R or KA = (GB mod R)A mod R or KA = (GB) A mod R or KA = GBA mod P.
KB = XB mod R or KB = (GA mod R)B mod R or KB =(GA) B mod R or KB = GAB mod R.
Such that KA = KB = K.

3. For Encryption we use session key K with Plain text PT that will generate a new Cipher text CT Then send CT as the cipher text to the receiver and for decryption, calculate the plain text PT from the cipher text CT.

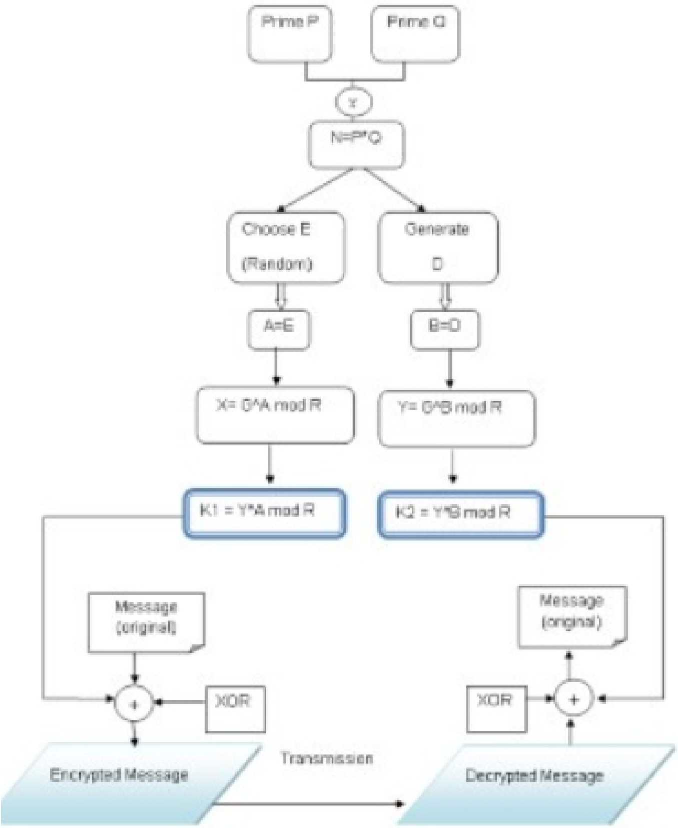


Figure 2: A Hybrid RSA &Diffie-Hellman [7]

4. PROPOSED WORK

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. So to improve the security, this scheme presents a new cryptography called Improved RSA (IRSA). IRSA is secure as compared to RSA as it is based on the factoring problem as well as decisional composite residuosity assumptions which is the intractability hypothesis. The scheme is an additive homomorphic cryptosystem; this means that, given only the public-key and the encryption of m_1 and m_2, one can compute the encryption of $m_1 + m_2$.

4.1 Improved RSA

IRSA4 is an asymmetric-key cryptosystem, meaning that for communication, two keys are required: a public key and a private key. Furthermore, unlike RSA, it is one way, the public key is used only for encryption, and the private key is used only for decryption. Thus it is unusable for authentication by cryptographic signing. Here „4“ indicates that this RSA uses four prime numbers to increased mathematical complexity for the attackers.

Following is a key generation algorithm for IRSA cryptosystem.

A. Key Generation Algorithm:

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.
2. Compute $n = p * q$, $m = r * s$, $\varphi = (p-1) * (q-1)$ and $\lambda = (r-1) * (s-1)$.

3. Choose an integer e, $1 < e < \varphi$, such that $\gcd(e, \varphi) = 1$.
4. Compute the secret exponent d, $1 < d < \varphi$, such that $e * d \bmod \varphi = 1$.
5. Select an integer $g=m+1$.
6. Compute the modular multiplicative inverse: $\mu = \lambda\text{-}1 \bmod m$.
7. The public (encryption) key is (n, m, g, e).
8. The private (decryption) key is (d, λ, μ).

B. Encryption:

1. Let m be a message to be encrypted where $0<mesg< n$.
2. Select random r where $r < m$.
3. Compute ciphertext as: c=gmesg^e mod n * rm mod m2.

C. Decryption

1. Compute message: $m = (((c\lambda \bmod m2 – 1)/ m) * \mu \bmod m)d \bmod n$

4.2 Example of Improved RSA

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length. p=3, q=5, r=7, s=2
2. Compute $n = p \text{ x } q=15$, $m= r \text{ x } s=14$, $\varphi= (p-1) \text{ x } (q-1)=8$ and $\lambda=(r- 1) \text{ x}(s-1)=6$.
3. Choose an integer e, $1 < e < \varphi$ such that $\gcd(e, \varphi) =1$ e=7
4. Compute the secret exponent d, $1 < d < \varphi$, such that $e \text{ x } d \bmod \varphi =1$. d=7
5. Select an integer g=m+1. g=15
6. Compute the modular multiplicative inverse: $\mu=\lambda$ -1 mod m.μ=5 The public (encryption) key is (n, m, g, e) (15, 14, 15, 7)

The private (decryption) key is (d, λ ,μ) (7, 6, 5)

Encryption:

Plaintext s=5
Select random number r, where r < m. r=13
Compute cipher text as: c=gs^emodn *rm mod m2. c=15^78125 x 3937376385699289 mod 142
Now here onwards large calculations

Decryption:

Compute original message:

$m = (((c\lambda \bmod m2 – 1)/ m) * \mu \bmod m)d \bmod$

4.3 Proposed Algorithm

Moreover, Internet and Network applications have seen a tremendous growth in the last decade. As a result incidents of cyber attacks and compromised security are increasing. This requires more focus on strengthening and securing our communication. One way to achieve this is cryptography. Although a lot of work has been done in this area but this problem still has scope of improvement. In this paper we have focused on asymmetric cryptography and proposed a novel method by combining the IRSA4 and Diffie-Hellman in order to achieve more security called as Improved RSA with Diffie-Hellman using 4 prime numbers IRDH4.

Steps of this algorithm are as:

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.

Compute N = P * Q, M= R * S, φ= (P-1) * (Q-1) and λ =(R-1) * (S-1). Choose an integer e, 1 < e < φ, such that gcd (e, φ) = 1.
Compute the secret exponent d, 1 < d < φ, such that e * d mod φ =1. Select an integer G=M+1.
Compute the modular multiplicative inverse: μ = λ-1 mod m.
And put the value of e and d from above as secret number such that A=e and B=d.

2. Now calculate following as public number X=GAmod R
Y= Gbmod R

3. Calculate session key with formula
KA = YA mod R or KA = (GB mod R)A mod R or KA = (GB)B mod R or KA = GBA mod P.
KB = XB mod R or KB = (GA mod R)B mod R or KB = (GA)B mod R or KB = GAB mod R.
Such that KA = KB = K.

4. For Encryption we use session key K with Plain text PT that will generate a new Cipher text CT Then send CT as the cipher text to the receiver and for decryption, calculate the plain text PT from the cipher text CT.

Firstly to use Improved RSA each user must (privately) choose fourlarge random numbers P,Q,R and S to create his ownencryption and decryption keys. These numbers must belarge so that it is not computationally feasible for anyone tofactor N = P*Q,M=R*S. Next step is to generate E andD. After this we put E and D as inputs A and B to Diffie-Hellman and compute XA and XB , through which wegenerate session key KA and KB such that KA = KB = K.Then we XOR our input Plain text with the session key (K)for Encryption or to produce Cipher text and forDecryption again XOR Cipher text with session key (K) toproduce original Plain text.

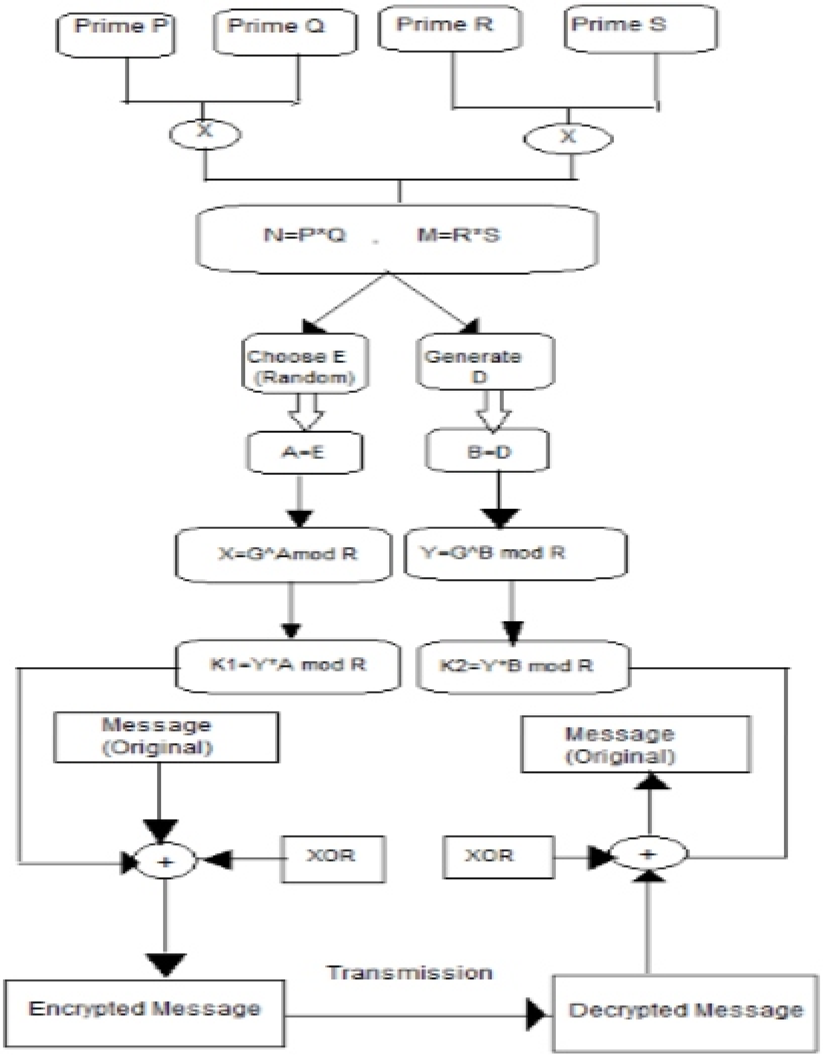


Figure 3: A Hybrid Improved RSA &Diffie-Hellman

5. COMPARATIVE STUDY

The Improved RSA cryptosystem is based on additive homomorphic properties and RSA cryptosystem, additive homomorphic scheme required four prime numbers, itwill be more difficult and take long time to factor dualmodulus, so one have to factor the dual modulus into its four primes to break the IRSA algorithm .If RSAwhich is based on single modulus, is broken in time x an dadditive homomorphic based on dual modulus, is brokenin time y then the time required to break IRSA algorithmis x*y. So the security of IRSA algorithm is increased ascompare to RSA algorithm and it shows that the IRSA algorithm is more secure for Mathematical attacks. As in IRSA double decryption is performed and unlikeRSA that is not only based on private key but also basedon the subset sum problem so one can"t break Improved RSA only guessing the private key only. So it shows that Improved RSA algorithm is more secure as compare to RSA for Brute force attack.

6. FUTURE WORK

The proposed approach will be of great use for the secure communication. It will be easy for user to send and receivemessages and files which are the most confidential to them. Presently, the usability of proposed Algorithm is given with veryfew concept and ideas which in future can be expand. Theefficiency in terms of time complexity can be revised forbetter working of algorithm. The key size for encryptionand decryption purpose can be reduces further. Currently the Algorithm is used for encryption and decryptionpurpose only. Further it can be used for digital signature generation.

7. CONCLUSION

Data confidentiality and security have become the prime aspects in today"s world of fast communication. Internet has played a vital role in bringing the world closer but at the same time has posed many challenges from data security and integrity point of view. After research across all the available material and techniques it was found that there is still lot work to be done in order to ensure data integrity. Keeping this in mind in this paper it has been tried to combine two of the best security algorithm RSA and Diffie-Hellman. Further we proposed a novel method, to strengthen the security aspect, by comparing both these algorithms and providing with the best of these two algorithms. It mainly concentrates on asymmetric cryptography by combining the IRSA and Diffie-Hellman in order to achieve more security called as Improved RSA with Diffie- Hellman using 4 prime numbers IRDH4. Moreover, still this area is continuous evolving and needs more work to be done on continuous basis.

8. REFERENCES

[1] *Yi Chen, Hong Chen, Hongqian, Chen, Xianchen Cheng-"Research on Data Encryption Techniques for Distributed Interactive Simulation Network", International Conference on Computer Application and System Modeling, IEEE 2010.*

[2] *Subhasis Mukherjee1, MaynulHasan, Bilal Chowdhury, Morshed Chowdhury-" Security of RFID Systems - A Hybrid Approach", 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, IEEE 2011.*

[3] *Kirtiraj B Hatele, Prof. Amit Sinhal, Prof. Mayank P Athak-"A Novel Approach to the Design of a New Hybrid Security Protocol Architecture", International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), IEEE 2012.*

[4] *Lili Yu, Weifeng Wang, Zhijuan Wang-"The Application of Hybrid Encryption Algorithm in Software Security", Fourth International Conference on Computational Intelligence and Communication Networks, IEEE 2012.*

[5] *Smita P. BansodVanita M. Mane Leena R. Ragha-" Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity", International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India, IEEE 2011.*

[6] *Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan-"Hybrid Crypto HardwareUtilizing Symmetric-Key & Public-Key Cryptosystems", International Conference on Advanced Computer Science Applications and Technologies, IEEE 2012.*

[7] *Shilpi Gupta , Jaya Sharma-"A Hybrid Encryption Algorithm based on RSA and Diffie- Hellman", International Conference on Computational Intelligence and Computing Research, IEEE 2012.*

[8] *William Stallings, Cryptography and Network Security Principles and Practice, fifth Edition, Pearson publication.*

[9] *Vishal Garg, Rishu, Improved and Diffie Hellman Algorithm for Network Security Enhancement, Int.J. Computer Technology &Applications, Vol 3 (4), 1327-1331.*

[10] *Ravi Shankar Dhakar, Amit Kumar Gupta-" Modified RSA Encryption Algorithm", 2012 Second International Conference on Advanced Computing & Communication Technologies,IEEE 2012*

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

-

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.

The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Note