International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 3091-3105

Redefining And Reassignment Of Trust Worthiness For Devices In Mobile Grid

Grantej Vinod Otari[1*], Dr. V. R. Ghorpade[2] And Dr. S. H. Dhanani[3]

[1]*shivaji University, Kolhapur, India.*
[2]*bharati Vidyapeeth's College Of Engineering, Kolhapur, India.*
[3]*k.I.T.'S College Of Engineering, Kolhapur, India*

Abstract

Mobile Technology And Grid Technology Can Be Combined Together To Provide A Distributed Collaborative Environment In The Form Of Mobile Grid Network, Where The Resources Can Be Shared Securely, Transparently And Cooperatively To Perform The Task Or A Job Efficiently And Reliably. The Resources In Such Mobile Grid Network Are Highly Dynamic, Heterogeneous And Open In Nature. This Makes The Network Vulnerable To Active And Passive Attacks Made By Selfish And Malicious Nodes In The Network. Detecting Such Malicious Nodes And Preventing Them To Selfishly Participate In The Network Is The One Of The Most Critical Security Service. This Security Service Can Be Implemented By Developing A Comprehensive Trust Management System. The Proposed Trust Management System In This Paper Is Based On Fuzzy Lattice Concept. The Proposed Model Classifies The Mobile Nodes Based On Their Trust Value As Highly Trusted, Average And Less Trusted. The Node With The Trust Value Below The Threshold Is Considered As Malicious Node And Prevented From Participating In The Network. Evaluating The Results Of Analysis Show That The Proposed Trust Model Using Fuzzy Lattice Method Provides Comparatively More Efficient Results In Terms Of Trust Computation Time And Resources Utilized To Compute The Trust Such As Battery, Cpu Etc.

Keywords: *Mobile Gird, Trust Management, Fuzzy Lattice*

1. Introduction

The Device Trust Architecture Is A Security Framework, Which Demonstrates How Trust Can Protect The Devices And Digital Services In Mobile Grid Network. This Is Achieved By Providing Security Services Implemented Within A Protected Framework And This Can Be Used From The Boot Process Of The Device Operating System (Os) To The Application Layer.

Why Is The Device Trust Architecture Needed?

The Devices Connected In The System Are Expanding Rapidly. Present Devices And Their Types Are Participating In A Variety Of Different Grid Platforms; Different Types Of Os Are Being Devised And Various Digital Services Are Hosted By These Devices. Not Every Device Is Safe Enough To Protect It From Threats And Attacks. Given The Fragile Nature Of Information Collected And Shared By These Devices, There Is A Major Risk Of Threats Across The Entire Ecosystem In Mobile Grid Network. For Successful Performance Of Digital Services [1][2]:

– Provider Of The Grid Service Needs To Trust That Devices That Are Gathering And Forwarding Data Related To Services Are Completely Secured, And Up-To-Date For Potential Attacks.

– Manufacturers Of Devices Need To Support A Variety Of Operating Systems, Securely Join Several Platform Providers And Allow Services Providers To Obtain The Right Level Of Secure Services[21].

– There Are Several Different Types Of Devices That Providers Of Grid Network Need To Safely Enroll In Various Security Services. End-To-End Data Integrity Is Necessary For Your Business Model From Legitimate Devices; If You Can't Trust The Data Source, Big Data Is Worthless. There Must Therefore Be A Preference For The Cooperation Of The Main Players In Securing Digital Infrastructure, Otherwise The Mobile Grid Ecosystems Will Not Reach Their Full Potential, And Big Data Infringements May Become A Standard [22].

ISSN: 2005-4238 IJAST

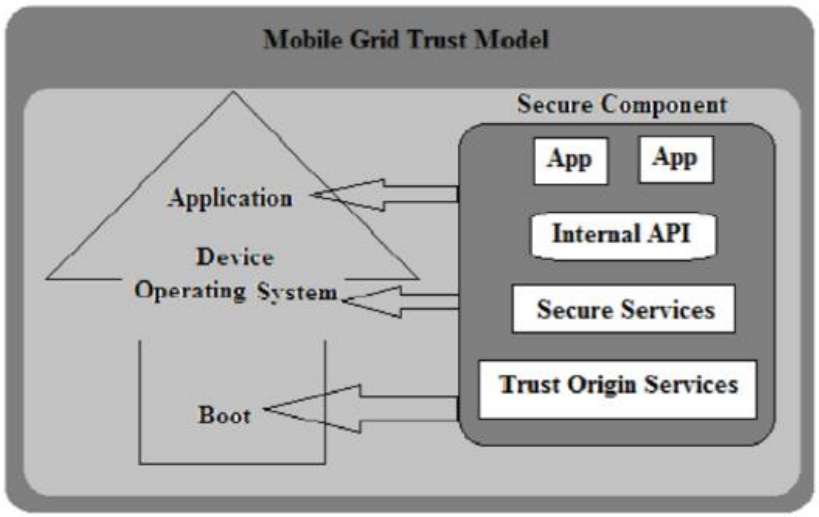

Figure 1. Device Trust Architecture Framework

2. Trust Necessity

2.1. Trust Architecture Framework

The System Trust Architecture Framework Enables Seamless Interaction Between Stakeholders, Regardless Of Business Or Device Type, When Integrating Secure Digital Services. The Integrity Of Data And Data Source Protection (I.E. Endpoint Device) In Is Vital To The Quality Of Service Provided By The Mobile Grid Applications [23].

2.2. Is Trust Important?

A. For Companies Producing Devices

In The Past Decade, Many Global Companies Have Taken Advantage Of The Digitalization Of Infrastructure To Seek Out New Routes On The Market. As Demand From The Customers And Industry Increases For Digital Services, A Broader Range Of Devices Such As Smartphones And Tablets Provide Access To Digital Services. A Real Security Test Is Required In This Complex Landscape. Device Vendors Confirm That They Will Provide Trustworthy, Reliable Services That Allow Service Providers To Use Their Devices Positively To Run Services Securely, Provide Safe Data Management And Delivery Of Digital Services To End-Users[21].

An Established Series Of Trust Provides Compatibility Of Secure Service Delivery Within A Device. It Enables Device Manufacturers To:

1. Ensure Their Devices Can Be Securely Entered Into The Grid Platforms;
2. Provide Assurances That Their Devices Can Securely Support Various Device Os;
3. Enable End To End Data Privacy / Secure Communications;
4. Maintain Secure Remote Updates For Device Services;
5. Protect Critical Edge Calculations.

B. For Grid Platform Providers

In An Associated Community, The Grid Platform Providers Have Turned Out To Be Immovably Settled As An On-Screen Character Who Bears A Stage That Empowers End-Clients And Providers To Collaborate And Oversee Exchanges. There Are Different Instances Of These New Biological System Players: For Example, Mobile Phone And Tablet App Stores (E.G., Google Play Store); Consumer Online Shopping Sites (E.G., Amazon, Alibaba).

ISSN: 2005-4238 IJAST

The Safe End-Client And Gadget Verification Are Additionally Typically Required, To Ensure That The Supplier Is Communicating With The Proposed Gadgets And Group Of Onlookers.

2.3. Trust Definition, Metrics And Properties Of Trust

Trust Is A Characteristic Of A Device That Is A Representation Of Level Of Satisfaction Of Different Devices In The System And Is For The Most Part Created In Light Of Relationship Encounters With Them At A Specific Time.

Trust Metrics:

Trust Evaluation Is Based On Various Metrics And Different Ways. A Few Models Use Ceaseless Or Discrete Numbers To Quantify The Trust. For Example, Trust Can Be Represented By Continuous Values In The Range [0, 1] Or Discrete Values In The Range [1, 1]. Threshold-Based Approaches Are Also Used To Measure Trust. Trust Metrics Are Probability Based, Fuzzy Based, Similarity, Mobility, Context-Based Features Like Energy, Hop Distance, Signal Strength, Etc [22].

Trust Estimation:

Properties Of Trust In Grid:

(A) A Hypothesis That All Nodes In The Grid Are Always Cooperative And Will Give True Feedback Should Not Be Considered By Trust Evaluation Model.

(B) Definition Of Trust Should Be In An Adaptable Way Without The Overhead Of Final Calculation And Communication.

(C) Trust Is Not Static, And It Is Dynamic.

(D) Trust Is Relative

(E) Trust Is Not Certainly Transitive.

(F) Trust Is Distorted And Unequal.

(G) Trust Is Context Dependent

Trust Evaluation Can Be Done Using The Following Paradigm:

Centralized Paradigm: A Central Server Estimates The Trust Of All Other Nodes In The Network.

Distributed Paradigm: Every Node Estimates The Trust Of Every Other Node In The Network.

Trust Evaluation Can Be Done Using The Following Paradigm:

Trust Management

The Following Are The Trust Management Phases:

- Trust Dissemination
- Trust Accumulation
- Trust Forecast

Trust Dissemination: To Evaluate The Trust Of A Device Consumes Lots Of Resources Of A Node Incurring The Cost Of Calculation And Communication. These Resources, Especially In The Mobile Grid, Can Be Limited. This Rate Of Resource Utilization For Reevaluation Of Trust Can Be Reduced By Propagating The Trust In The Network. This Trust Transmission Takes Place Between Peers In The Network. Trust Dissemination Is Based On The Transitivity Property Of The Trust. The Most Important Part Of Trust Dissemination Is The Participation And Cooperation Of All The Nodes In The Network For Transferring The Trust Information [15, 16].

Trust Accumulation: As Trust Is Generated Through The Network, Multiple Accounts Of Trust For A Single Device Will Be Received By A Device. The Distinct Values Of Trust Will Be Required To Be Accumulated In Order To Calculate The Final Value Of Trust. Trust Accumulation Depends On The Composability Property Of The Trust. Trust Path Is Composed Of The Sequence Of Nodes That Transfer The Trust Information About The Target Node To The Requestor [15, 16].

ISSN: 2005-4238 IJAST

Trust Forecast: Trust Forecast Is A Method Of Predicting The Trust Of A Node Based On Its Present And Historical Behavior And Also The Reputation Received From Other Nodes [15]. Real Life Models Might Include An Ebay Seller That Builds A Reputation Score Of The Summary With Some Successful Transactions Of Low-Value Goods. The Seller Might Be Highly Considered Regarding Reputation To Provide Excellent Service During Transactions, But Then Degrade That Service When Selling A Particular Item Of A Significantly Larger Value. In The Trust Forecast System, A Requirement Should Be Entertained Such As If A Transaction Is Failed, But The System Predicts That It Would Be Successful Results In A False Positive, Whereas A Successful Transaction That Is Predicted To Be Dangerous By The System Is A False Negative. [26]

2.4. Trust Calculation

Trust Relations Are Essential Way Of Doing Business Today. The Success Of Business Depends Significantly On The Level Of Trust In Business Relations, Whether Employees Or Co-Workers Inside Or Clients And Partners Outside The Business.

The Challenge Is Having A Conceptual Architecture And Analytical Way Of Assessing And Learning Trust. In The Absence Of The Proper Framework For Estimating Trust, There Is No Actionable Way To Change Our Trustworthiness[26].

The Trust Model Is Thus The Foundation Of Our Relationship: A Deconstructive, Logical Model Of Trustworthiness That Can Be Directly Agreed Upon And Applied To Help Oneself And One's Organization.

The Four Variables

There Are Four Objective Variable In The Trust Equation To Estimate Trustwor- Thiness. These Four Variables Are Expressed As Credibility, Reliability, Intimacy, And Self-Orientation

Credibility

Determines The Degree Of Believability Of An Entity. It Is The Quality Of Being Trusted And Believed In.

Reliability

Determines The Degree Of Consistency In Trustworthiness. It Is The Quality Of Being Consistently Trustworthy.

Intimacy

Determines The Degree Of Confidentiality. It Is The Quality Of Being Confidential And Maintaining Privacy.

Self- Orientation

Determines The Degree Of Selfishness. It Is The Quality Of Being Selfish And Self-Focused.

We Consolidate These Variables Into The Following Equation To Evaluate Trust [24]:

$$Tq = (C + R + I)/S$$

Where The Trust Quotient (Tq) Denotes A Number That Scales Your Trustworthi- Ness With Respect To The Four Variables. Larger The Value Of The Variables In The Numerator Greater Is The Trustworthiness.

The Most Critical Variable In The Above Trust Equation Is Self-Orientation Which Is Used As The Denominator. A Self-Oriented Seller For Example Will Focus Primarily On Its Own Benefits Rather Than Focusing On The Benefits Of The Customer. Such A Selfish Seller Will Be Considered Less Trustworthy.

ISSN: 2005-4238 IJAST

3. Related Work

Qiyi Han[3] Has Suggested Hfstrust A Hierarchical Fuzzy Scheme That Computes The Local Trust By Extracting Information From Local Logs On Past Interactions. This Model Also Gathers Information From Other Peers In The Network In Order To Estimate Indirect Trust Using Peer Recommendations. Finally, A Global Trust Metric Has Been Developed And Used For Taking Decision By Combination Of The Local Trust Metric And Recommendation Metric.

In Order To Help Cloud Customers To Trust The Cloud Service Providers, Frtm [4] A Trust Model Based On Reputation Using Fuzzy Logic Inferences Is Proposed To Deal With Uncertain And Inadequate Information In Cloud Trust Reports. The Frtm Model Performs Fuzzy Inference On Various Properties Of Perceived Services Such As Quality Of A Service, Cost Of Service, Delivery Time Etc. The Results Of The Fuzzy Inference Are Then Used To Assess The Customer Satisfaction, Which In Turn Can Be Used To Compute Local Trust Of The Cloud Service Provider. Finally Frtm Collects The Local Trust Scores From All The Cloud Customers To Generate Global Trust Score For A Cloud Service Provider Using Fuzzy Inference Rules. The Author Sunil Kumar Et Al.[20] Has Proposed A Framework For Trust Management In Cloud Based On Fuzzy Logic. The Proposed Model Consists Of Two Main Modules. Registration Management Service (Rms) Module Collects The Information Of All The Cloud Service Providers And The Services Provided By Them. Trust Management Service (Tms) Module Uses The Fuzzy Logic To Compute The Trust Value Of The Cloud Service Provider Considering Four Parameters: Security, Availability, Cost And Performance. Ftcp [6], A Fuzzy-Based Trust Computational Protocol Is Proposed To Alleviate Black Hole Attack In Aodv Protocol In Manet. Ftcp Is A Weighted Binary Relational Model That Computes The Direct Trust Value Of A Neighbouring Node Using Four Trust Parameters: Packet Forwarding Rate, Battery Consumption, Buffer Consumption And Number Of Requests For Connection. The Performance Of Ftcp Is Analysed Using Three Parameters: Packet Delivery Ration, Average End- To-End Delay And Throughput. Tcfl [7], A Trust Mechanism Is Examined Where Methodology Used Is Fuzzy Logic In Which Trust Is Evaluated On The Basis Of Previous Action Of Sensor Nodes. Trust Values Are [0,1] That Are Computed. The Advantage Of This Model Is Using Fuzzy Reduction Unsure And Unspecific Data Can Be Calculated. Limitations Include Centralized Plan Is Appropriate For Most Wsns. Memory Requirement To Cache Earlier Activity Of Sensor Nodes Is The Complexity Of This Model.

Rfsn [8] Trust Mechanism Is Studied Where Probability Theory And Bayesian Network Is Used As Methodology Where Watchdog Is Utilized To Scan Adjacent Nodes Activity. Trust Values Consist Of [0,1] Where Implementation Issue And The Energy/ Memory Overhead Of Rfsn Are Examined. Trust Calculation Specified Without Single Point Defect Is The Advantage Of This Model. This Model Can Enhance Security, Whereas System Robustness Cannot Be Enhanced Which Is The Limitation. Bayesian Computation Needs Memory And Calculation Complexity.

Weighing Technique Is Used By Plus[9] For Measuring Trust On The Basis Of A Specific Citation And Recommendation. Trust Values Are In The Range [0,1] And The Proposed Model Is Evaluated For Various Malicious Attacks And Overhead Involved In Computation And Communication. The Benefit Of This Trust Model Is That It Detects Malicious Nodes Consistently, While The Drawback Is High Convergence Time. Plus Does Not Suit High-Traffic Wsns. Complexity In The Implementation Of A Number Of Citation Protocols Is The Computational Complexity Of This Trust Mechanism. Additional Memory Required To Store Citations.

Fuzzy Theory And Theory Based On D-S Evidence Is Used By Nbbte [10]. Trust Is Measured Based On Behavior Of Nodes Transferring Packet. The Trust Values Are [0,1] Used To Test The Impact Of Malicious Nodes. The Benefit Is That The Protection Of The Network Is Combined And Time Differences Are Defined. The Trust Measurement Involves An Overhead Of Energy And Time Because Of Collaboration And Coordination With Neighbor. Memory Consumptions Are Often Increased With The Network Density.

Zhengwang Ye[11] Presented A Well-Organized Dynamic Trust Evaluation Model (Dtem) For Wireless Sensor Networks (Wsns) In Which It Provides An Efficient And Dynamic Method For

ISSN: 2005-4238 IJAST

Measurement Of Trust By Dynamically Modifying The Weights And The Parameters Of The Direct And Indirect Trust. Global Trust Is Determined By Assigning And Combining Complex Weight For Direct And Indirect Trust. An Updated Mechanism Is Finally Presented Through A Sliding Window Centered On The Persuaded Weighted Central Operator In Order To Increase Versatility. The Parameters Can Be Dynamically Adjusted To The Specific Needs Of The Network And The Interactive History Windows Can Be Used To Dynamically Update The Direct Value Of The Confidence. Results From The Simulation Suggest That An Appropriate Dynamic And Attack-Resistant Trust Assessment Model Has Been Developed. The Approach Proposed Blends Current Approaches With Dynamic Trust Model In Which Multiple Malicious Attacks Are Better Defended.

Pedro B. Velloso [12] Introduces A Human-Based Model That Creates Trust Between Nodes Within An Ad-Hoc Network. Trust Depends On Previous Experiences And On Reference From Peers. The Recommendation Exchange Protocol (Rep) Permits Nodes To Share Their Neighbours' Recommendations. Without The Need For Global Trust Awareness, The Solution Proposed Is Well Suited For Broad Networks, While Reducing The Amount Of Messages And The Use Of Resources. Also The Liars Gathered In The Network Decrease The Impact Of Colluding Attacks. An Essential Part Is The Maturity Of The Relationship, Which Makes The Presented Model For Mobile Scenarios More Effective. In A Single Hop Network Simulation, The Accuracy Of The Proposed Model Is Seen. It Is Also Possible To Study Mobile Multi-Hop Networks, Which Offer The Advantages Of The Idea Of Maturity. Lastly, The Efficiency And Scalability Of The Rep Protocol Is Investigated. The Approach Proposed Shows That Rep Implementation Can Reduce Numbers Of Messages Significantly.

Fuzzy-Iot [18], Is A Fuzzy Based Security Solution To Mitigate On-Off Attacks And Contradictory Behaviour Attacks By Malicious Nodes In Cluster Based Iot Network. Fuzzy-Iot Uses Fuzzy Logic To Calculate The Trust Score Of The Nodes And Classify The Nodes As Trusted, Semi Trusted And Untrusted. The Direct Trust Scores Are Then Communicated To The Master Nodes In Each Cluster Which Then Computes Indirect Trust Scores. The Master Nodes In Each Cluster Then Send The Trust Scores To The Super Node In The Network. The Super Node Computes The Global Trust Score For Each Node. The Proposed Solution Uses Message Structure Based On Two Digit Hexadecimal Number To Detect Tampering Of The Message By Malicious Nodes During Communication In The Network.

Hongmei Liao[19] Worked On Trust That Changes Over Time. A Recent Behavioral Trust Model Using Fuzzy Logic Is Presented For Grid Environment. Absolute Trust Can Be Achieved By Means Of Variable Weighted Fuzzy Logic Calculations, And Repudiation Can Be Procured By Deriving The Trust And Combining It. The Participation Of Experts Is Used To Create Simple And Flexible Rule Base. Malicious Advice Is Often Excluded And Punished In This Model During The Trust Transmission Process. The Simulation Results Show That Grid Components Can Be More Securely Used Using The Proposed Fuzzy Trust Model For Accessing The Resources Or Services.

Jose E. Fadul [20] Has Addressed The Utilization Of A Toolkit For Trust Management Which Provides A Vigorous And Configurable Enhanced Security System, Which Can Be Used To Effectively Enhance The Security In The Smart Grid Containing Untrustworthy (Malfunctioning) Devices. The Toolkit Merges A Reputational Trust With Network Flow Algorithms To Detect Deficient Security And/Or Communication Elements. The Results Of The Simulation Provide Support For The Proposed Toolkit For Trust Management.

A Research On The Grid Computing Used To Share Idle Or Available Resources For Solving Large-Scale Science Issues Has Been Carried Out By V. Vijayakumar [22]. In Such An Environment Security Is An Important Issue Of Concern. The Proposed Approach Is Analyzed With The Methods Implemented Earlier, Where Experimental Analysis Demonstrates Better Results For Selecting The Resources Securely Using Trust And Reputation. Also The Proposed Solution Guarantees Better Outcomes Than The Previous Methods For A Significant Number Of Malicious Nodes.

4. Proposed Methodology

ISSN: 2005-4238 IJAST

In Mobile Grid For Efficient Execution Of Jobs Nodes Need To Transmit Sensing And Control Data In An Open And Dynamic Sharing Environment. This Makes The Environment Highly Susceptible To Malicious And Selfish Attackers Spreading Harmful And False Messages In The System. To Prevent The Participation Of Such Malicious And Selfish Nodes In The Mobile Grid Network, It Is Inevitable To Evaluate The Trust-Worthiness Of The Participants. The Nodes With Low Trust Value Are Treated As Malicious And Prevented From Entering The Network. The Proposed Trust Management System Works In Three Phases: Direct Trust Calculation, Indirect Trust Calculation And Global Trust Calculation. The Proposed Model Identifies And Avoids Selfish Or Malicious Nodes From Participation In The Task And Improves The Efficiency Of Job Execution. Analysis Of The Proposed Model With The Existing Lightweight And Dependable Trust System Shows That The Rate Of Trust Examination Using The Proposed Model Improves By Up To 30% [13].

4.1. Fuzzy Lattice Trust System

Trust Models Based On Fuzzy Logic Utilizes A Rule-Based Method. The Fuzzy Rules Utilize The Semantics Of The Input And Output Variables To Describe The Nature Of The Inference System. The Expert Knowledge Is Generated In The Form Of If X Then Y Rules. The Rule Based Fuzzy Systems Are Inefficient When The Constraints Between The Objects Used For Classification Are Loose. The Rule-Based Fuzzy Framework Allows Multi-Sequence Data To Be Introduced Only To Reduce The Cost Of Computation. Fuzzy Rules Require Expert Knowledge. The Method Does Not Require The Explicit Rule Description To Be Implemented With Adequate Knowledge Of The Classification Goal. Also With Increasing The Number Of Input Parameters, The Likelihood Of Trying Each Possible Combination Of Inputs Decreases.
In Contrast To The Fuzzy Logic Method, A Fuzzy Lattice Method Incrementally Computes The Same Intervals In Data Irrespective Of The Presentation Order And With Minimum Time Interval. In Addition, By Extracting Rules On Data, This Approach May Justify Its Results. This Can Also Be Useful For The Mining Of Data And Rules Involving Various Data Types. Additional Studies Can Be Carried Out On This Method, Both To Boost Efficiency And To Reduce The Number Of Regulations.

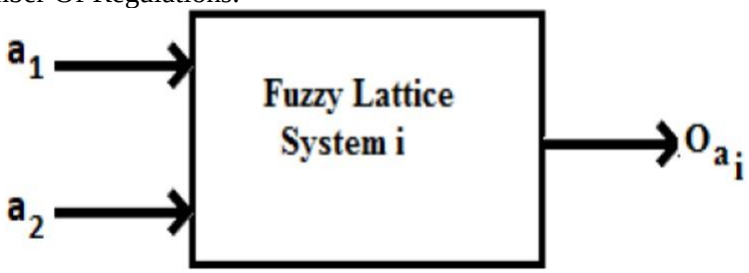

Figure 2. Fuzzy Lattice System

The Proposed Model Works In Four Stages [17]

i. **Linguistic Inputs (Trust Components):** The Trust Model Uses The Fuzzy Lattice System As Shown In Figure 2. The System Uses M Input Variables Which Describe Attributes Or Parameters Of The Node In The Network. Some Primary Attributes For Trust Calculation Indicating The Capability Of The Mobile Node To Perform The Task Or Job In The Grid Network Are As Follows.

Table 1: Trust Attributes

Notation	Trust Estimation Parameter
A1	Percentage Of Cpu
A2	Percentage Of Battery

ISSN: 2005-4238 IJAST

A3	Amount Of Storage
A4	Amount Of Bandwidth
A5	Job Success Rate
A6	Task Completion Time
A7	Online Time Rate
A8	Operating System

The Output Of The Fuzzy System Describes The Three Levels Of Trust Values: Low (L), Average (M), And High (H). Trust Can Be Assessed At Three Levels As Shown In Figure 3 [25]: Direct Trust Between Neighboring Nodes, Indirect Trust Between Non-Neighboring Nodes, And Past Trust From The Historical Behavior.

Direct Trust

Each Peer Maintains A Record Of Trust Factors Whenever It Interacts With All Other Peers In The Network. The Direct Trust Dt(X,Y) Between A Trustor Node X And A Trustee Node Y At The Time (T) Is Estimated By

$$DT = \frac{\sum_{a_1=1}^{n_1}\sum_{a_2=1}^{n_2}\cdots\cdots\sum_{a_m=1}^{n_m} V_{i=1}^{n_m} O_{a_i}}{\sum_{a_1=1}^{n_1}\sum_{a_2=1}^{n_2}\cdots\cdots\sum_{a_{m-1}=1}^{n_{m-1}} V_{j=1}^{n_{m-1}} O_{a_j}}$$

where

$$O_i = V_{k=1}^{3}\left\{max\left\{\Lambda_{j=1}^{n}[1-\mu_k^j(x_j), 1-\mu_k^j(x_{j+1})], \beta_k^i(x)\right\}\right\}$$

where

$$\beta_k^i(x) = min\left\{\beta_k^i(x_j), \beta_k^i(x_{j+1})\right\}$$

Where N_m Describes Numbers Of Levels Having M Attributes Or Parameters;
O_a Is The Output, Of Each Fuzzy System At The I^{th} Level.

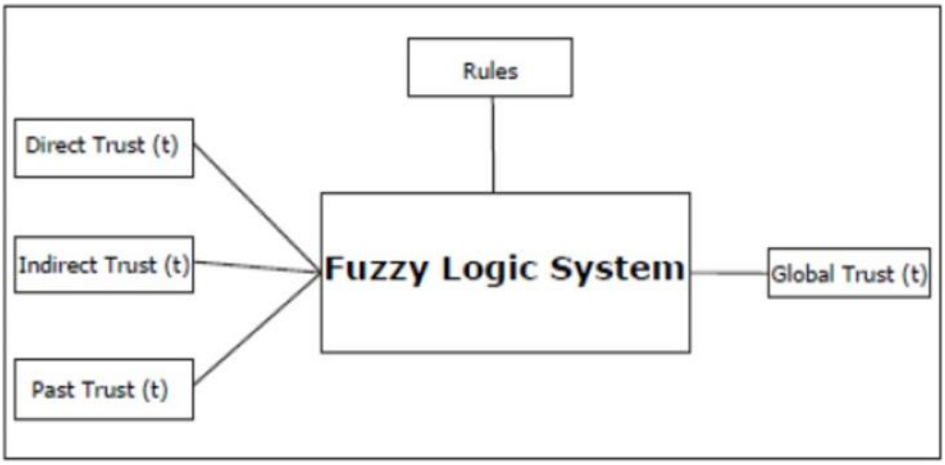

Figure 3. Fuzzy Logic Trust Model For Grid

Indirect Trust

Each Node, In The Model Periodically Collects The Direct Trust Values From All Other Nodes In The Grid. Indirect Trust Is One To One Process Where The Device Computes The Indirect Trust Within Each Node. The Model Uses To Fill The Matrix With The Node's Feedback As Shown In [25].

ISSN: 2005-4238 IJAST

$$Feedback = \begin{bmatrix} DT_{1,1} & \dots & \dots & DT_{1,n} \\ .. & \dots & \dots & .. \\ .. & \dots & \dots & .. \\ DT_{n,1} & \dots & \dots & DT_{n,n} \end{bmatrix}$$

The Proposed Model Uses A Generic Approach Used By Social Platforms Like Facebook, Twitter Etc That Is Based On Recommendations And The Principle Of Psychology. The Nodes Within The Network Decide Whom To Trust Based On The Recommendation From The Mutual Friend On The Network. When A Recommentation Of The Node Is Received From The Recommender, It Is Used To Establish A Trustful Relationship Between The Trustor And The Trustee And The Trust Value Between The Trustor And The Trustee Shall Not Be Higher Than Between The Recommender And The Trustee.

$$RT_{i,j} = \frac{\sum_{k=1}^{n} DT_{i,k} * RT_{k,j}}{\sum_{k=1}^{n} DT_{i,k}}$$

Past Trust

Historical Behavior Of Each Node Is Used By The Model To Keep Track Of Each Node Because That Could Create A Threat To The Network. In Order To Escape From Punishment A Selfish Nodes Could Act Like A Normal And Malicious Alternatively. The Past Trust [17] Tpast At The Time (T) Is Estimated Using The Following Equation:

$$T_{past}(t) = \frac{\sum_{i=1}^{t-1} GT(i)}{t-1}$$

Ii. **Fuzzification Process:**

In This Process The Crisp Values Of The Trust Attributes Are Transformed Into The Linguistic Fuzzy Input Variables And Are Connected Using Logical And Operator. For Transforming The Crisp Input Values To Fuzzy Values The Model Uses A Triangular And Trapezoidal Membership Functions. The Model Uses Three Membership Functions Labeled By Three Fuzzy Numbers L, A, And H Indicating Three Levels Low, Average And High Respectively.
Membership Function For The Fuzzy Numbers L, A, And H [25] Are Given By:

$$M_L(x) = \begin{Bmatrix} 0, & x > c_1 \\ \frac{c_1 - x}{c_1 - c_2}, & c_2 \le x \le c_1 \\ 1, & x < c_2 \end{Bmatrix}$$

$$M_A(x) = \begin{Bmatrix} 0, & x \le b_1 \\ \frac{x - b_1}{b_2 - b_1}, & b_1 < x \le b_2 \\ \frac{b_3 - x}{b_3 - b_2}, & b_2 < x < b_3 \\ 0, & x \ge b_3 \end{Bmatrix}$$

$$M_H(x) = \begin{Bmatrix} 0, & x < a_1 \\ \frac{x - a_1}{a_2 - a_1}, & a_1 \le x \le a_2 \\ 1, & x > a_2 \end{Bmatrix}$$

Iii. **Fuzzy Inference Rule-Base:**

The Membership Function Used For Estimating Global Trust (Gt) Is As Shown In The Figure 4. The Node With Low Trust Value Is Treated As Malicious And Node With High Trust Value

ISSN: 2005-4238 IJAST

Behaves Normal And Is Trusted. The Fuzzy Sets Defined Above Are Used As Input To Calculate The Global Trust (Gt) Values Using Fuzzy Inference Rule Base As Shown In Table 2. The Number Of The Input Variables Is Three In This Method, And Each Variable Takes Three Values. Thus, The Total Number Of Rules, With All Possible Combinations, Is 27.

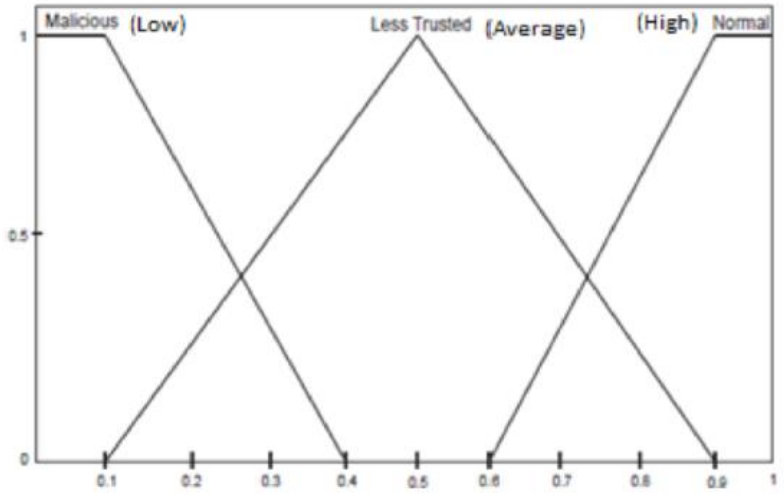

Figure 4. Membership Functions For Global Trust

Table 2: Fuzzy Rules For Global Trust (Gt)

If Dt Is	And Rt Is	And Pt Is	Then Gt Is
L	L	L	L
L	L	H	L
L	H	L	L
H	L	L	L
L	H	H	H
H	L	H	H
H	H	L	H
L	L	A	L
L	A	L	L
A	L	L	L
L	A	A	A
A	L	A	A
A	A	L	A
A	A	A	A
H	H	H	H

Iv. **Defuzziftcation**:
The Defuzzification Process Transforms The Resulting Fuzzy Values To Crisp Values Using Middle Of Maximum (Mom) Technique. This Technique Is Efficient For Mobile Grid Nodes Having Resource Constraints. The Function Gets The Average Value Of The Maximum Range Of Rules Aggregation.

5. Result And Discussion

Trust Evaluation System Thus Act As An Effective Decision Support System That Intends At Creating Trust By Calculating The Trust Degree Of The Device, In Turn, To Help Users In

ISSN: 2005-4238 IJAST

Taking A Proper Decision On Specific Feedback Or Going Forward To Perform A Transaction. Here, A Trust Management System Is Proposed Which Strives To Calculate The Trust Index Of The Device According To Its Subjective Marking From Various 9 Options. The Proposed Trust System Also Calculates The Global Trust Reliability Score Of The Node For Its Different Aspects And Generates The Trustworthiness Of The Device On Given Feedback. Finally, The System Produces The Rating.

The Performance Of The System Is Analyzed Using A Test Bed Consisting Of Different Smartphone Devices Like Samsung Galaxy On7 Pro, Xiaomi Redmi Note- 11, Motorola G3 Etc. The Category Of Devices Has Been Selected With Various Fea- Tures To Perform And Analyze This System. Observations Have Been Calculated For Five Different Devices So That Analysis Can Be Done Efficiently And Accurately. The Primary Challenge Was To Collect The Initial Genuine Trust Value Because It Forms The Base Of Our Future Trustworthiness Score. We Compared The Proposed Fuzzy Lattice-Based Trust Management System With The Existing Hierarchical Fuzzy Logic Based Trust System Hfstrust [14] And Analyzed The Performance Of Both The Systems Based On Response Time, Energy Consumed And Cpu Utilization.

Each Algorithm Is Executed For 5 Rounds. The Details Of Each Round Are As Shown In Table 3.

Table 3: Details Of Rounds Of Execution

Round Number	Number Of Nodes
1	5
2	10
3	15
4	20
5	25

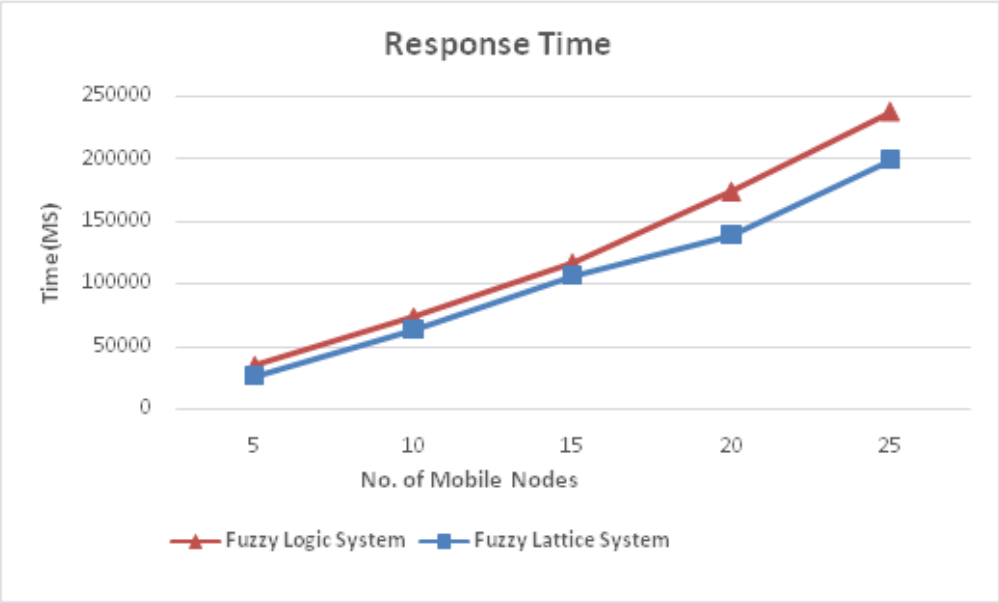

Figure 5. Response Time

As Figure 5 Shows, The Time Taken For Fuzzy Hfstrust Hierarchical System Execution Is More For All The Datasets Compared To The Proposed Trust Model Based On Fuzzy Lattice Because The Number Of Comparisons Is Reduced In The Proposed Model. In Addition, Battery Consumption And Cpu Utilization Of The Proposed Fuzzy Lattice Trust Model Is Less As Compared To Hfstrust As Shown In Figure 6 And Figure 7.

ISSN: 2005-4238 IJAST

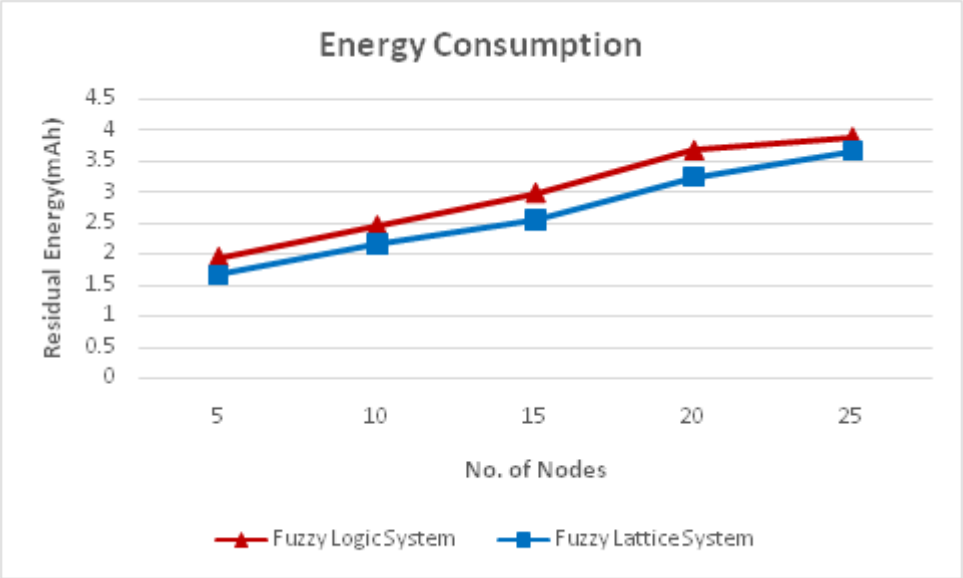

Figure 6. Energy Consumption

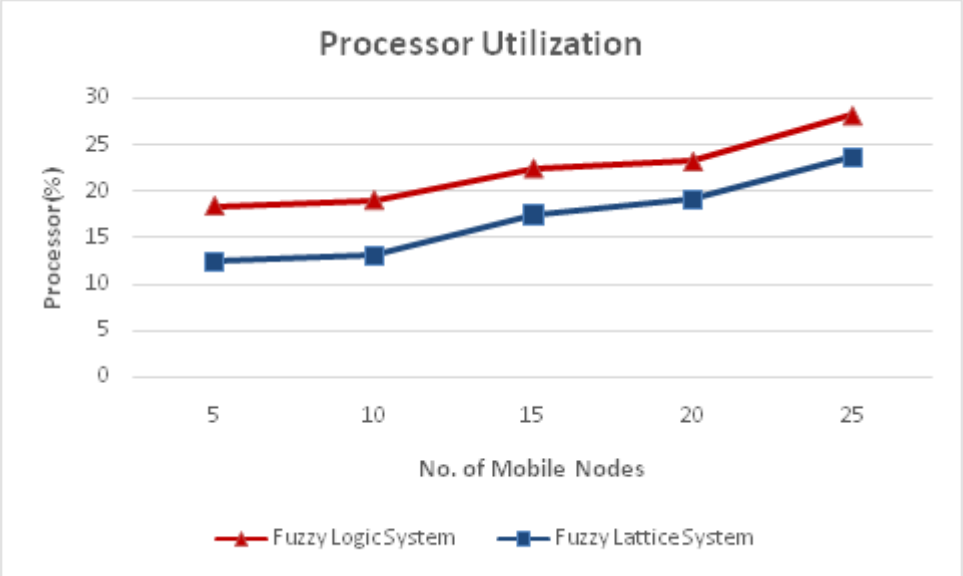

Figure 7. Cpu Utilization

Each Algorithm Is Executed For Five Rounds. During Each Round, Both The Algorithms Are Executed Ten Times To Evaluate The Trust Index Of 5 Devices. The Precision And Accuracy Of The Algorithm Is Shown In Contingency Table 4 And Represented Graphically In Figure 8.

Table 4: Average Precision

Tp	Tn	Fp	Fn	Recall	Precision
90	2	3	5	0.9474	95
90	3	5	2	0.9783	92
90	2	5	3	0.9677	93
85	4	9	2	0.977	87
85	5	5	5	0.9444	90

ISSN: 2005-4238 IJAST

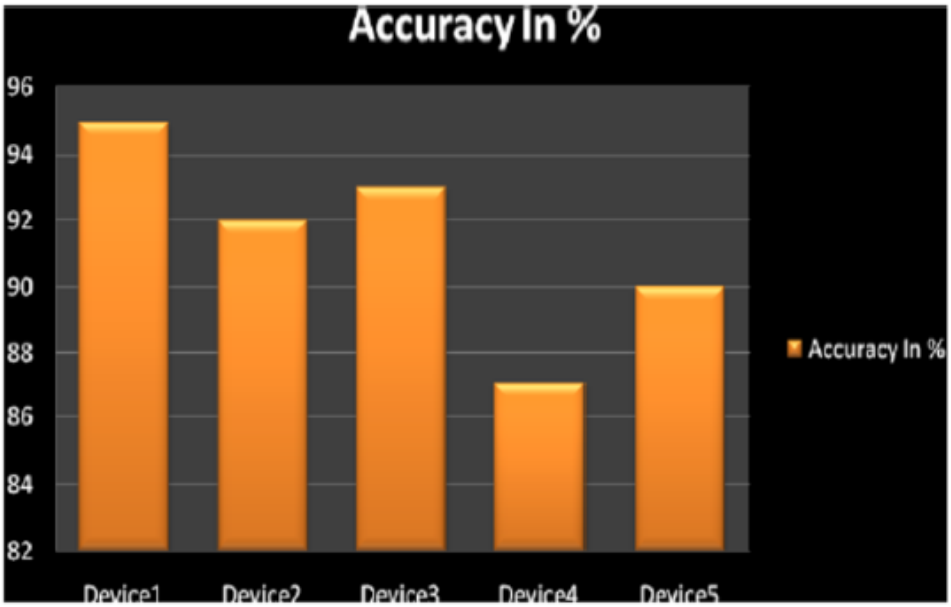

Figure 8. Average Accuracy

6. Conclusion And Future Scope

Fuzzy Lattice Is A Novel And Efficient Method For Evaluating The Trust Worthiness On The Devices In The Mobile Grid Network. The Proposed Trust Model Evaluates The Trust Index Of The Nodes Using The Parameters Based On The Capability To Perform The Task And The Log Of Past Interactions. Our Trust Model Also Considers The Recommendations From The Peers In The Network To Derive Indirect Trust Of A Node. Experimental Evaluation Proves Fuzzy Lattice To Be An Effective And Alternative Technique For Trust Estimation As Compared To Most Of The Existing Trust Models Based On Traditional Method Of Fuzzy Logic. The Proposed Model Outperforms The Existing Fuzzy Logic Based Models In Terms Of Computation Time And Consumption Of Precious Mobile Resources Such As Battery And Cpu With Improved Accuracy And Precision.

References

[1] J. Jiang And Y. Qian, “Distributed Communication Architecture For Smart Grid Ap- Plications,” Ieee Communications Magazine, Vol. 54, No. 12, Pp.60–67, 2016.

[2] J. Jiang And H. Sun, “Performance Assessment Of Distributed Communication Archi- Tectures In Smart Grid,” In Proc. Ieee 83rd Vehicular Technology Conference (Vtc Spring), Pp. 1–5, 2016

[3] Qiyi Han, Hongwen, Gang Feng, Binwu, Mengyin Ren, Self-Nominating Trust Model Based On Agglomerative Fuzzy Systems For Peer-To-Peer Networks, Springer Peer-To-Peer Networking And Applications, Volume 9, Issue 6 , Pp 020–1030, November 2016.

[4] Xu Wu, A Fuzzy Reputation-Based Trust Management Scheme For Cloud Com- Puting, International Journal Of Digital Content Technology And Its Applica- Tions(Jdcta), Volume6, Number 17, September 2012

[5] Sunil Kumar, Sumit Mittal, Manpreet Singh,Fuzzy Based Trust Manage- Ment System For Cloud Environment,Advances In Science And Tech- Nology, Research Journal,Volume 10, No. 30, Pages 32–37, June 2016.

[6] Ashish Kumar Jain, Vrinda Tokekar And Shailendra Shrivastava,Security Enhance- Ment In Manets Using Fuzzy-Based Trust Computation Against Black Hole At- Tacks,© Springer Nature Singapore Pte Ltd. 2018.

ISSN: 2005-4238 IJAST

[7] Ing-Ray Chen And Jia Guo, Dynamic Hierarchical Trust Management Of Mobile Groups And Its Application To Misbehaving Node Detection, Ieee International Conference On Advanced Information Networking And Applications (Aina), 2014.

[8] Hui Xia1, Zhiping Jia1, Lei Ju1, Xin Li1, Youqin Zhu2, A Subjective Trust Man- Agement Model With Multiple Decision Factors For Manet Based On Ahp And Fuzzy Logic Rules, Ieee/Acm International Conference On Green Computing And Communications, 2011.

[9] Pedro B. Velloso, Rafael P. Laufer, Daniel De O. Cunha, Otto Carlos M. B. Duarte, And Guy Pujolle, Trust Management In Mobile Ad Hoc Networks Using A Scalable Maturity-Based Model, Ieee Transactions On Network And Service Management, Vol. 7, No. 3, September 2010.

[10] Ji Guo , Alan Marshall, Bosheng Zhou , A New Trust Management Framework For Detecting Malicious And Selfish Behaviour For Mobile Ad Hoc Networks, Inter- National Joint Conference Of Ieee Trustcom-11/Ieee Icess-11/Fcst-11, 2011.

[11] Zhengwang, Ye And Wen, Tao And Liu, Zhenyu And Song, Xiaoying And Fu, Chong- Guo, "An Efficient Dynamic Trust Evaluation Model For Wireless Sensor Networks", Journal Of Sensors, Pp. 1-16, Vol. 2017, Doi. 10.1155/2017/7864671, Issue 10, 2017.

[12] P.B.Velloso And R.P.Laufer And D.D.O.O.Cunha And O.C.M.B.Duarte And G.Pujolle, "Trust Management In Mobile Ad Hoc Networks Using A Scalable Maturi-Tybased Model", Journal Ieee Transactions On Network And Service Management, Doi.10.1109/Tnsm.2010.1009.I9p0339, Pp.172-185, Vol.7, No.3, Issn.2373-7379, Is- Sue Sep, 2010.

[13] Daki, Houda & El Hannani, Asmaa & Aqqal, Abdelhak & Haidine, Abdelfattah & Dahbi, Aziz, Big Data Management In Smart Grid: Concepts, Requirements And Implementation. Journal Of Big Data. 4. 10.1186/S40537-017-0070-Y, 2017

[14] Qiyi Han, Hongwen, Gang Feng, Binwu, Mengyin Ren, Self-Nominating Trust Model Based On Agglomerative Fuzzy Systems For Peer-To-Peer Networks, Springer Peer-To-Peer Networking And Applications, Volume 9, Issue 6, Pp 020–1030, Novem- Ber 2016.

[15] N. Labraoui, A Reliable Trust Management Scheme In Wireless Sensor Networks, In Proceedings Of The 12th International Symposium On Programming And Systems (Isps). Ieee, Pp. 1–6, 2015.

[16] M. Wazid, A. Katal, R. S. Sachan, R. Goudar, And D. Singh, "Detection And Pre- Vention Mechanism For Blackhole Attack In Wireless Sensor Network," In Proceedings Of The International Conference On Communications And Signal Processing (Iccsp). Ieee, Pp.576–581, 2013.

[17] Aljawharah Alnasser, And Hongjian Sun, Senior Member, Ieee, A Fuzzy Logic Trust Model For Secure Routing In Smart Grid Networks.Doi 10.1109/Ac- Cess.2017.2740219, Ieee Access.

[18] Alshehri, M.D., Hussain, F.K., "A Fuzzy Security Protocol For Trust Management In The Internet Of Things (Fuzzy-Iot)", Computing Vol. 101, Pp. 791–818, 2019.

[19] Hongmei, Liao Andwang, Qianping And Li, Guoxin, "A Fuzzy Logic-Based Trust Model In Grid",Doi.10.1109/Nswctc.2009.218,Pp.608-614,Vol.1, Issue 05, 2009.

[20] Fadul, J.E. And Hopkinson, K.M. And Andel, Todd And Sheffield, C.A.,A Trust-Management Toolkit For Smart-Grid Protection Systems, Journal Power Delivery, Ieee Transactions On,Doi.10.1109/Tpwrd.2013.2289747,Pp.1768-1779,Vol.29, Is- Sue 08, 2014.

[21] Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons Of Machine Learning And Security Methods ", 2019.Http://Gujaratresearchsociety.In/Index.Php/ Jgrs, Issn: 0374-8588 ,Volume 21 Issue 4

ISSN: 2005-4238 IJAST

[22] Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, " Machine Learning & Its Classification Techniques ",International Journal Of Innovative Technology And Exploring Engineering (Ijitee) Issn: 2278-3075, Volume-8 Issue-9s3, July 2019.

[23] Subramaniyan, Sridhar And Ramachandran, Baskaran,Trust Based Scheme For Qos Assurance In Mobile Ad-Hoc Networks,Journalcorr, Doi 10.5121/Ijnsa. 2012.4108,Vol.Abs/1202.1664, Issue 01, 2012.

[24] Varadarajan, Vijayakumar And Banu, R., Performance Analysis In Secured Grid Resource Selection Based On Trust And Reputation, International Journal Of Com- Puter Applications, Pp. 28-32, Vol. 31, Doi. 10.5120/3790-5218, Issue 10, 2011.

[25] Https://Globalplatform.Org/Wpcontent/Uploads/2018/07/Introduction-To-Device- Trust-Architecture-20july2018.Pdf

[26] Atul B Kathole, Dr.Dinesh N.Chaudhari, " Fuel Analysis And Distance Predication Using Machine Learning", 2019 ,International Journal On Future Revolution In Computer Science & Communication Engineering, Volume: 5 Issue: 6.

[27] 24. Https://Trustedadvisor.Com/Why-Trust-Matters/Understanding- Trust/Understanding-The-Trust-Equation

[28] 25. Aljawharahalnasser, And Hongjian Sun,"A Fuzzy Logic Trust Model For Secure Routing In Smart Grid Networks", Ieee Access,Volume 5, 2017, Pp. 17896-17903.

ISSN: 2005-4238 IJAST