TRUST AND PRIVACY CONCERNS IN MOBILE CROWD SOURCING

Report submitted in partial fulfillment of the requirement for the Degree of

Master of Technology

In

Computer Science & Engineering

Under the Supervision of

Dr. Hemraj Saini

By

Shailja Joshi (162201)

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY

(Established by H.P. State Legislative vide Act No. 14 of 2002)
P.O. Waknaghat, Teh. Kandaghat, Distt. Solan - 173234 (H.P.) INDIA
Website: www.juit.ac.in
Phone No. +91-01792-257999
Fax: +91-01792-245362

CERTIFICATE

This is to certify that project report entitled "**Trust and Privacy Concerns in Mobile Crowdsourcing**", submitted by **Ms Shailja Joshi** in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been made under my supervision.

This report has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Date:

Dr. Hemraj Saini
Associate Professor
Department of Computer Science and Engineering,
JUIT, Solan (H.P.)

ACKNOWLEDGEMENT

I want to convey my deep and genuine appreciation to my research supervisor, **Dr. Hemraj Saini** (Associate Professor), Jaypee University of Information Technology Waknaghat, Solan for providing me this chance. His valuable guidance and direction throughout this research was of utmost importance. He taught me the art of conveying the research work as clearly as possible. It was a privileged to have worked under him.

I would also like to express my gratitude to faculty member **Dr. Geetanjli Rathee** and PhD scholar **Shivi Sharma** for their valuable suggestion and support.

I would also like to thank my HOD (Computer science and Engineering & Information Technology) **Prof. Dr. Satya Prakash Ghrera** and also the student coordinator of M.Tech **Dr. Pardeep Kumar** (Associate Professor) for their help and support. I would have not been able to complete the research without their permission to use the resources and facilities available in the institute.

I am extremely thankful to my parents for their unconditional support be it financially, emotionally or morally. Their divine teachings and prayers will always remain with me as a shield.

I am extending my gratitude to my batch mates of M.Tech (class of 2018) for their help during my research work.

Date: **Shailja Joshi**

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

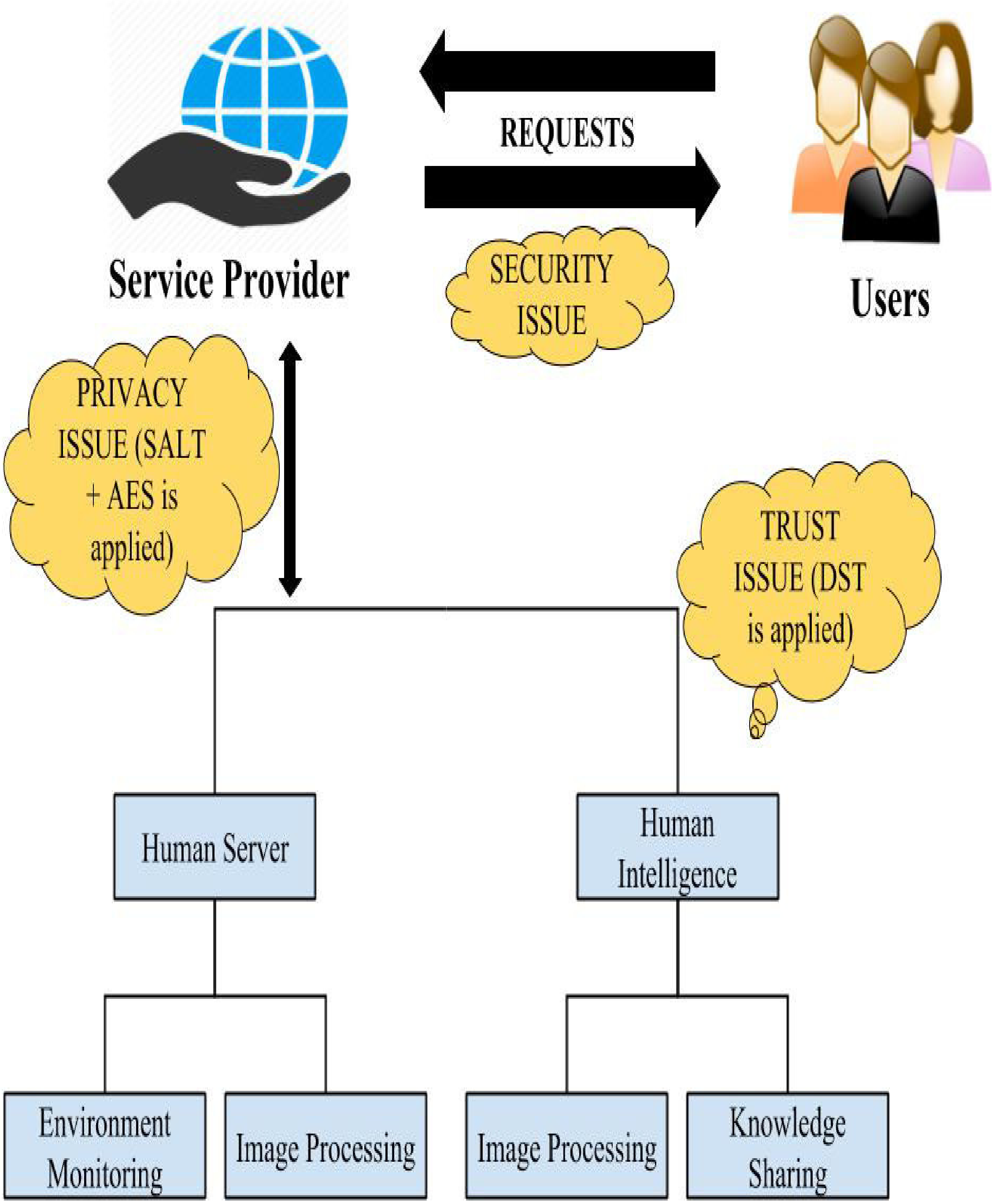
Crowdsourcing is a method or a technique in which solution to a problem is given by dividing the problem into a number of small tasks and then assigning them to different users. This assignment is done by broadcasting the task or the problem to the crowd. Mobile Crowdsourcing (MCS) has evolved as an appropriate method for collecting the data or finding solution of a broadcasted task where the mobile phone users can perform the task anytime and anywhere as they wish. These tasks are taken by the mobile users and are solved according to their perspective and ability. The crowdsourced task is the one which requires human skills and is difficult for a computer to solve. Therefore, mobile devices play an important role in Mobile Crowdsourcing (MCS) by being both service consumer and service provider at the same time. MCS holds many advantages like human capability, cost-efficiency and information sharing. These advancement leads to the concern of:

1. **Trust:** The quality of data that is shared among the users may sometimes be of poor quality or it can be said that the information is not trustworthy.
2. **Privacy:** Exploitation of users' personal information due to non- restricted usage of data by any third party applications.

Therefore the motive of this research is to deal with these two issues of "trust" and "privacy" in Mobile Crowdsourcing and provide secure and trustful environment for the users or workers of crowd sourcing.

1. The characteristics of MCS are analyzed and DST (Dempster–Shafer Theory) algorithm is proposed as a solution to achieve the goal of trust in MCS system.
2. SALT cryptography with AES (Advanced Encryption Standard) is proposed as a solution for ensuring the privacy. SALT is used as a noise with the user's personal information so that only the valid users will be able to access the information.

The obtained results are in well support of the proposed solutions.


Service Provider
REQUESTS
Users
SECURITY ISSUE
PRIVACY ISSUE (SALT + AES is applied)
TRUST ISSUE (DST is applied)
Human Server
Human Intelligence
Environment Monitoring
Image Processing
Image Processing
Knowledge Sharing

CHAPTER 1
OVERVIEW OF CROWDSOURCING

1.1 INTRODUCTION

The word "Crowdsourcing" was coined by Jeff Howe and Mark Robinson in the year 2005 that depicts a developing model in which online laborers were used for critical thinking task. Later on it was widely considered as an appropriate method for programming structures [1]. Now days, crowdsourcing as a model is rising day by day and its outcome is a composition of both human and machine. As per the universally accepted definition, crowdsourcing stands for an organization that conducts an open call for a particular project to an undefined network of users/ workers [1].

Smartphone's as we know are an amalgamation of two very distinctive set of features which are packed into one device. The smart phones technology these days is everything apart from being just a phone. It is equipped with delicate sensors like GPS, accelerometer, camera etc while also enabling a device to relay and receive information using multiple radios like wifi, cellular etc. The combination of both enables a user to perform the task of collecting a data and then distributing or relaying it easier. This has enabled us to get into a new era where there is a whole new concept of mobile crowdsourcing [2].

Looking at the Indian market, the number of mobile user has increased dramatically in past decade. As we know fixed line telephone was once a must have for Indian households which has now been almost completely replaced by mobile communication technology. According to a survey the percentage of mobile phone users in India in the year 2017 was 33.4% and the percentage of population using internet on mobile devices was 23.93%. These figures point towards an exponential growth in the scope for mobile crowdsourcing technology among the Indians. With increase in demand for social networking through mobile devices and the development of concepts like participatory detection, Mobile

Crowdsourcing (MCS) can possibly help to handle new issues related to constant information gathering and coordination among countless users [3].

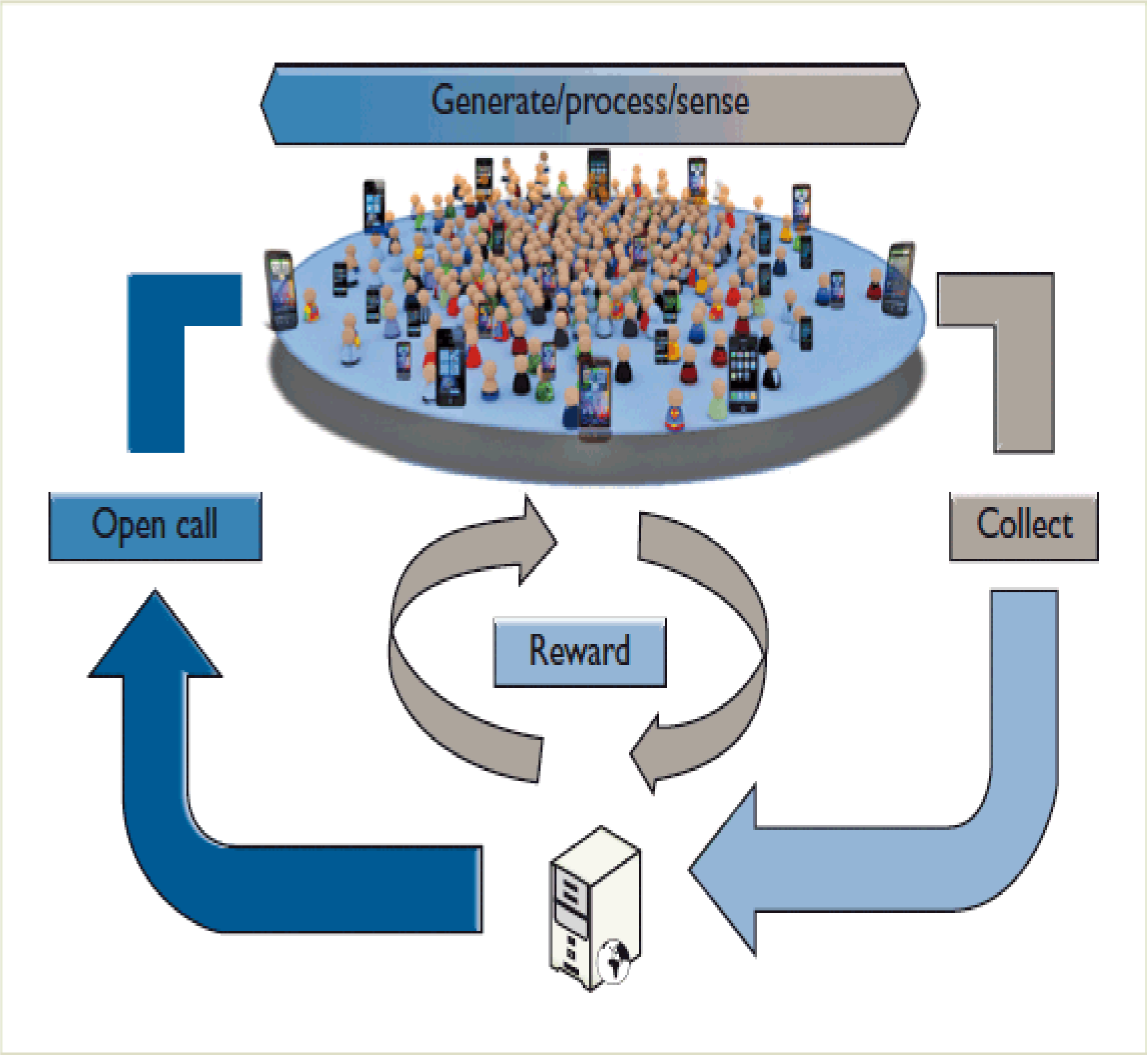


Figure 1.1 Crowdsourcing with Smartphone's

As of late, MCS detection is a progressing field of research where advanced mobile devices are turning into a vital part of individuals' day to day existence [2]. On the other hand MCS faces some critical issues, such as security, privacy, and trust during the transmission, informationvgathering or sharing of the data among each other. Therefore, the main focus of this paper is mainly concerned with:

1. **“Trust Issue”** where the quality of data that is shared among the users may sometimes be of poor quality or it can be said that the information that is shared by the user not trustworthy. To begin with this, trust issues in mobile crowdsourcing are vitally concerned with ‘Laborer Trust’ and ‘Information Trust’. For example, it sometimes happens that laborer out of their selfish reasons mislead by giving biased or false information. Incidents like these defeat the very purpose of mobile crowdsourcing [4].

2. **“Privacy Issue”** where the crowdsourcing workers personal detail may be misused. Therefore, it becomes important to protect the details of workers for which the idea of data hiding is used [5]. The data hiding or information hiding is a concept which is used in wide range of applications like text, audio, video etc. The goal of information hiding can be achieved through various techniques like cryptography, steganography etc.

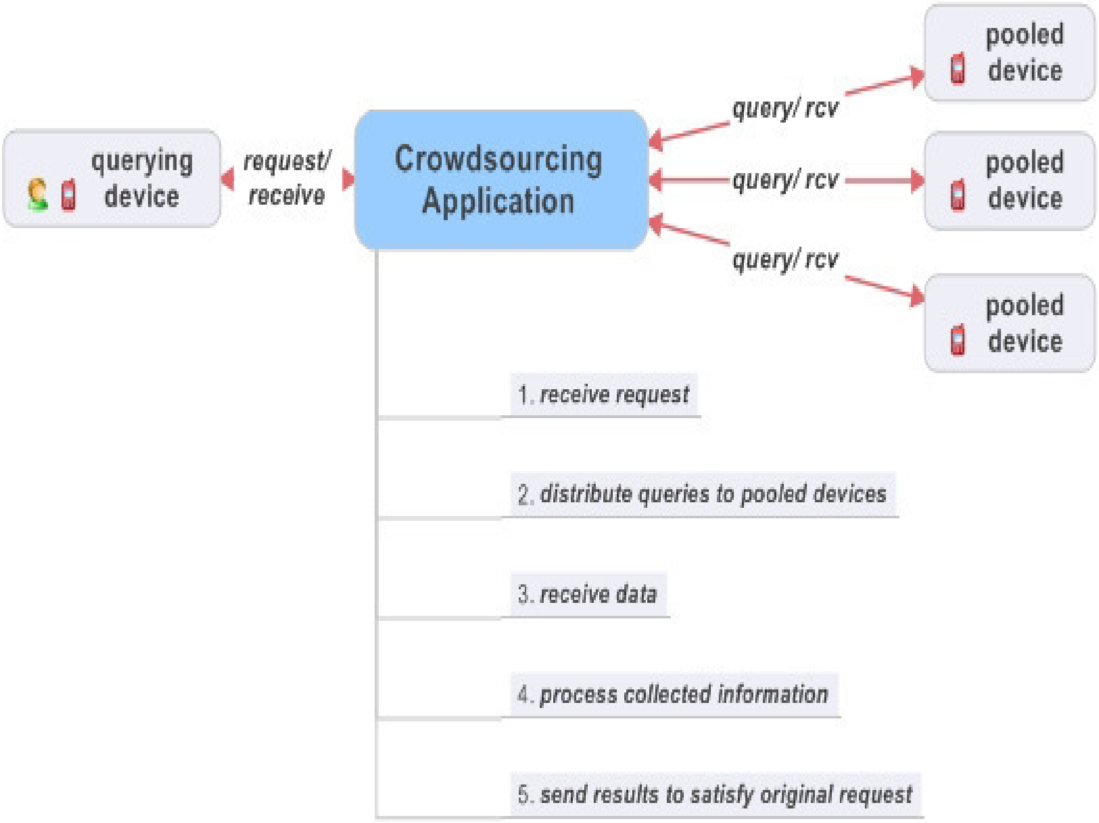

querying device
request/ receive
Crowdsourcing Application
query/ rcv
query/ rcv
query/ rcv
pooled device
pooled device
pooled device
1. receive request
2. distribute queries to pooled devices
3. receive data
4. process collected information
5. send results to satisfy original request

Figure 1.2 Mobile Crowdsourcing Architecture

1.2 BRIEF HISTORY

Even though the term "crowdsourcing" came to existence in year 2005, but its practice had started long back.

1. The Longitude Prize in 1714

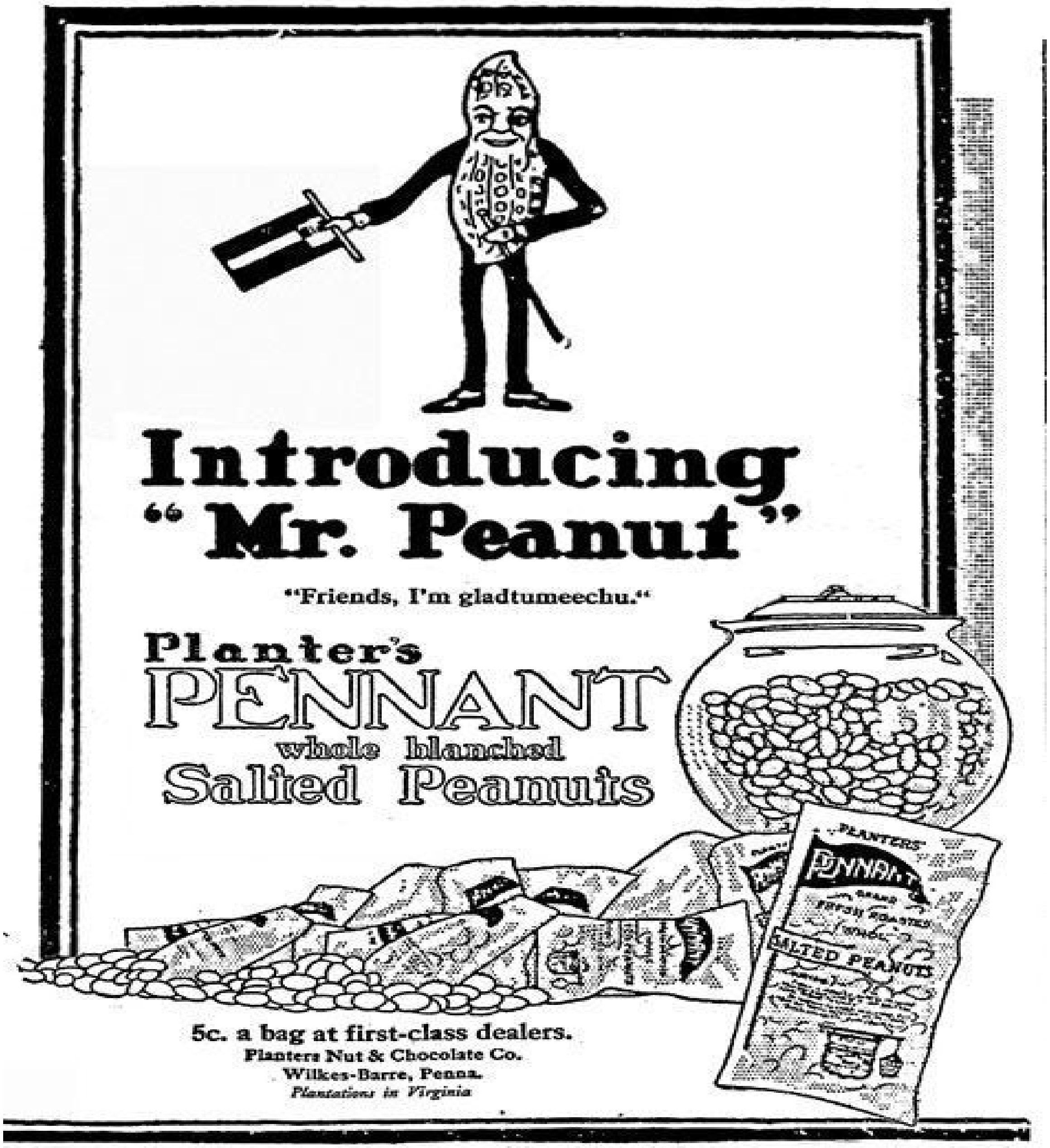
"Longitude Problem" was the condition in which sailing became difficult and hazardous leading to the death of 1000 or more seamen every year. The British government in year 1714 decided that they have to find solution to this problem as early as possible. Therefore, they decided that whoever will come up with the solution for this problem he will be awarded £20,000. The winner of this contest was John Harrison who was the son of a carpenter; he invented a pocket watch which was accurate, vacuum sealed and he named it as 'marine chronometer'. This was the first crowdsourcing method which clearly showed that when given an opportunity solution can come from anywhere.

2. Oxford English Dictionary in 1884

The Oxford English Dictionary editor in a newspaper published an open call in the year 1884. The open call was that anyone can give quotations for normal or ordinary words and can also give quotations that have words that were new, out of date or distinct.

3. Planters Peanuts in 1916

Planters Peanuts were the first one who to record logo through crowdsourcing. This was done in the year 1916 and it is famous with the name Mr. Peanut mascot. The winner was Antonio Gentile a 14 year-old boy.



Introducing
"Mr. Peanut"

"Friends, I'm gladtumeechu."

Planter's
PENNANT
whole blanched
Salted Peanuts

5c. a bag at first-class dealers.
Planters Nut & Chocolate Co.
Wilkes-Barre, Penna.
Plantations in Virginia

Figure 1.3 Planters Peanuts Logo

4. Toyota Logo Contest in 1936

Just like Planters Peanuts, Toyota also organized a contest to redesign their logo in the year 1936. 27,000 entries were received out of which the winning logo was three Japanese katakana letters in circle meaning "TOYODA". This was later modified to "TOYOTA" by Risaburo Toyoda.

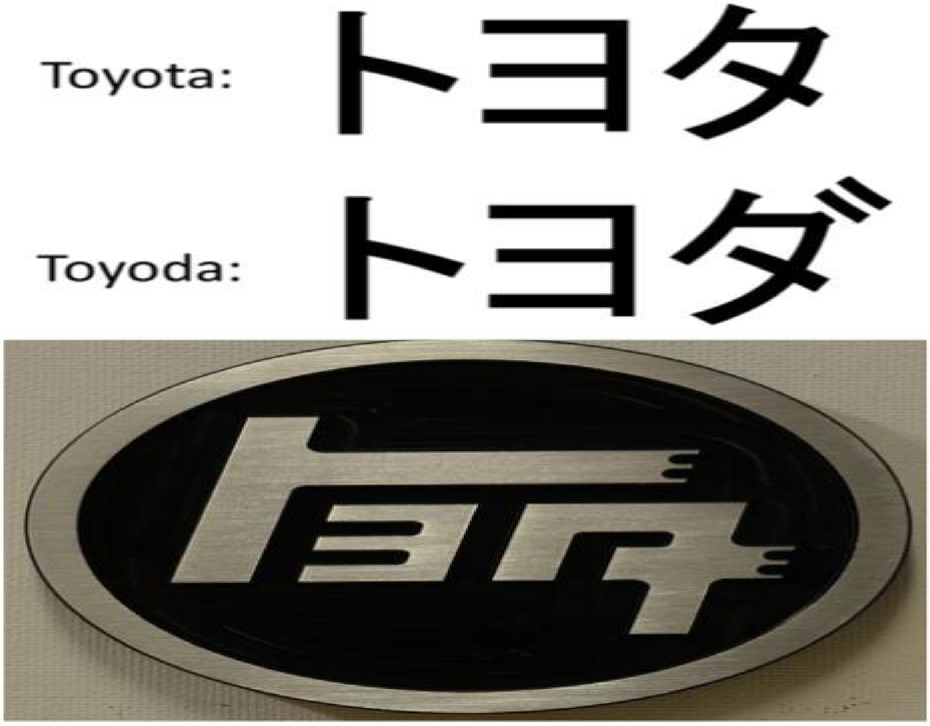


Figure 1.4 Logo of TOYOTA

5. **The Sydney Opera House in 1955**

   The premier of NSW (New South Wales) of Australia happened in the year 1955, a contest was ran by Joseph Cahill to design a building for Sydney's Harbour and the winning amount was £5,000. The winning design was among 233 entries from 32 countries.

6. **YouTube, Wikipedia in 2000 to 2006**

   YouTube a crowdsourced entertainment and Wikipedia the crowdsourced knowledge took-off during this period.

7. **American Idol in 2002 to 2006**

   Kelly Clarkson's career started with American Idol Season in the year 2002. Many other reality shows like So You think You Can Dance, Next Top Model, Master chef all crowdsourcing contests.

8. Crowdsourcing in 2006

Crowdsourcing was introduces on June 2006 in a magazine article which was together formed by J. Howe and M. Robinson.

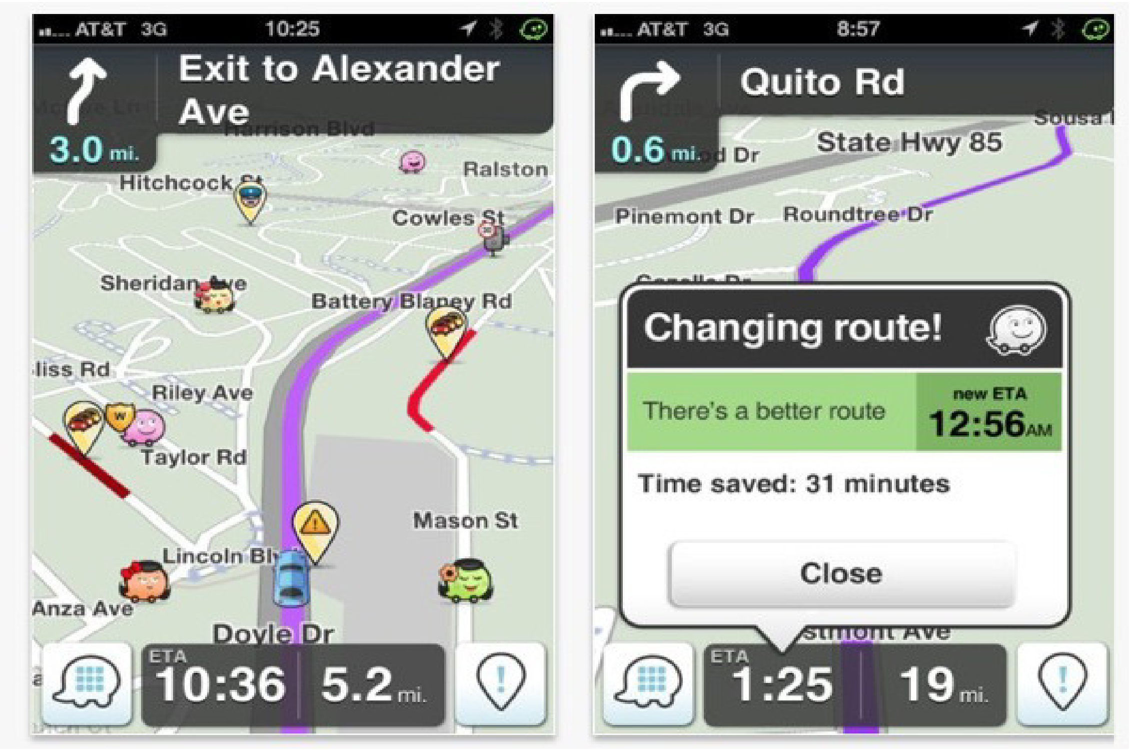
9. Crowdsourcing Explodes from 2006 to 2050

This period is and will be a rising phase of crowdsourcing nearly all start-ups depends on crowd.

1.3 APPLICATIONS

1. Maps and Traffic Information-(Waze)

This Waze application is a road map in which ‘n’ number of users are there and they keep on reporting the current situation of the road like how much traffic is there, an accident or construction work going on is also reported. Therefore saving the time.



Changing route!

There’s a better route

Time saved: 31 minutes

Figure 1.5 Waze Application View

2. Be My Eyes

This was a very useful application for “blind peoples”. In this if any blind user need assistance or any sort of help he/she may go for live video/audio call and the sighted users may help them if they want to.

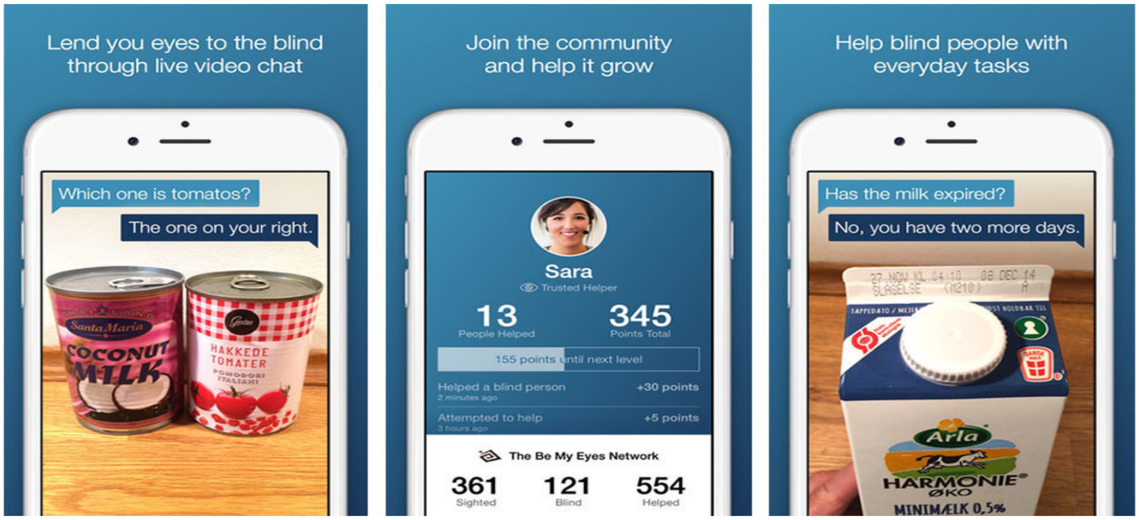
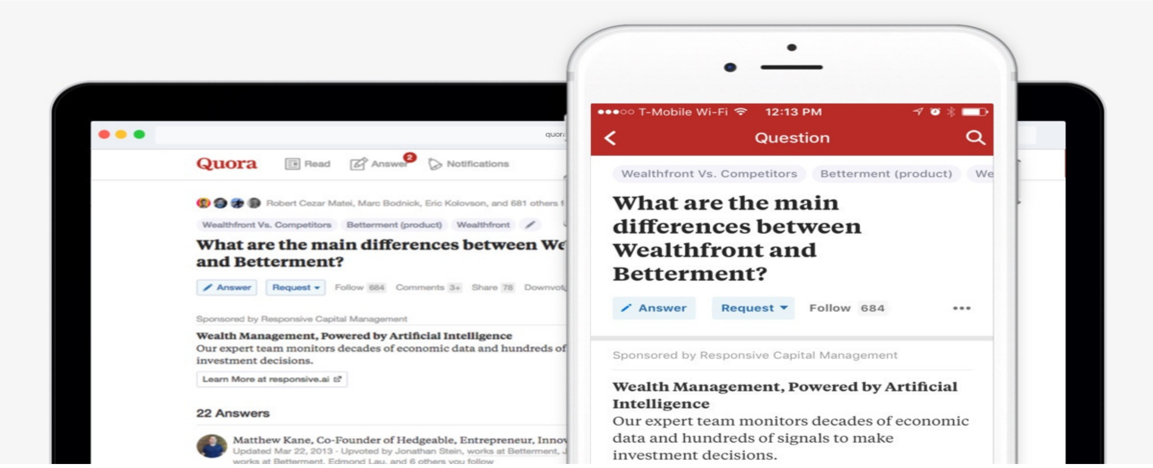


Figure 1.6 Be My Eyes Application View

3. Quora

Quora is knowledge sharing applications were you can put your query and experts will answer them. This is integrated with social applications therefore you can link your Facebook, Twitter and other social accounts.



What are the main differences between Wealthfront and Betterment?

Sponsored by Responsive Capital Management

Wealth Management, Powered by Artificial Intelligence
Our expert team monitors decades of economic data and hundreds of signals to make investment decisions.

Matthew Kane, Co-Founder of Hedgeable, Entrepreneur, Innov
Updated Mar 22, 2013 · Upvoted by Jonathan Stein, works at Betterment,

Figure 1.7 Quora Application View

4. Figure 1

This application can be considered as an Instagram application but just for doctors. In this all doctors add their discoveries as discuss it with other doctors. The thing that is kept in mind is that patient's privacy in protected.

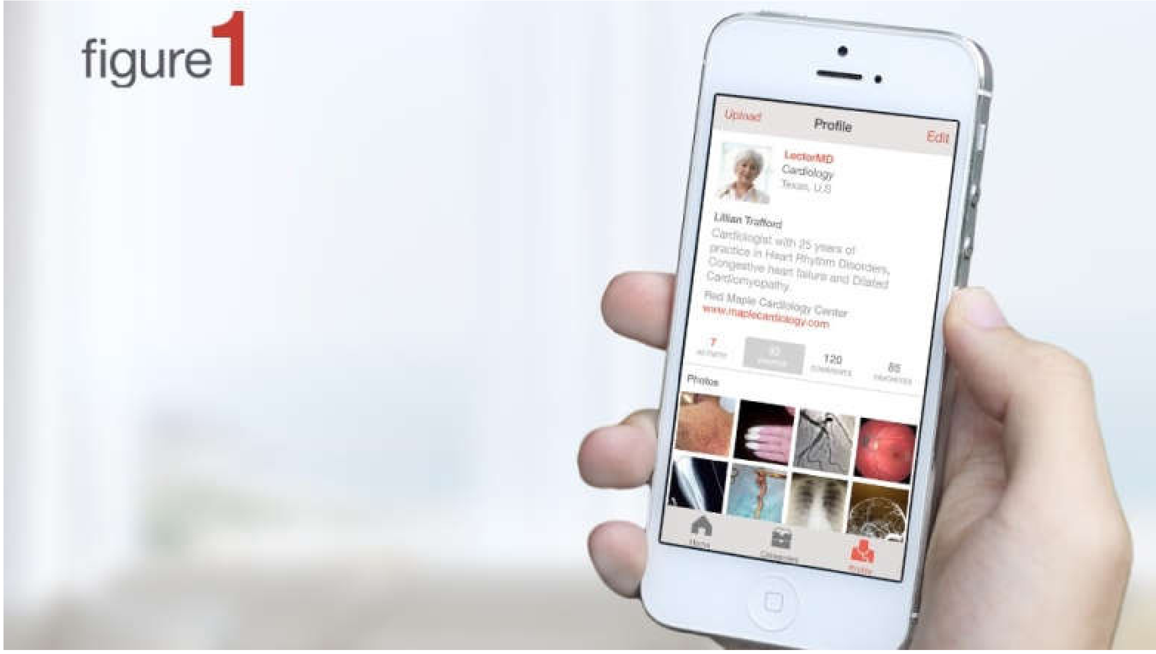


figure1
Upload
Profile
Edit
LectorMD
Cardiology
Texas, U.S
Lillian Trafford
Cardiologist with 25 years of practice in Heart Rhythm Disorders, Congestive heart failure and Dilated Cardiomyopathy.
Red Maple Cardiology Center
www.maplecardiology.com
7
120
85
Photos

Figure 1.8 Figure 1 Application View

CHAPTER 2
LITERATURE SURVEY

2.1 TRUST ISSUE

Various scientists/researchers have proposed number of papers and contributed to the development and widened the scope of mobile crowdsourcing technology.

H. Lin et al. [6] proposed wisdom of crowds so that risk could be identified and reduced. The proposed results included a questionnaire on supply chain and group of SMEs (Society of Manufacturing Engineers) rated those questions.

A. C. Weaver et al. [7] had effectively built up a collection of application (desktop web, mobile web, and standalone mobile). These applications were utilized for crowdsourcing data from clients who were taking part and then displayed that information so that the resident know about the wellbeing and welfare of their known individual in armed force.

Y. Liu et al. [8] created and analyzed an online learning algorithm for complex voting methods that ensured the performance of workers. This was the very first algorithm that analyzed the quality of labelers' online. The best set of labeling task were selected with O(log2 T) regret uniform in time. The results proposed were validated via both synthetic and real world AMT (Amazon Mechanic Turks) data.

J. Ren et al. [9] proposed a Social Aware Crowdsourcing with Reputation Management (SACRM) which was used in mobile sensing for the selection of participants that were well suited and rewarding them accordingly for the task they performed. For the selection process attributes that fit the set budget were taken into considerations like social, delay in performing task and reputation among the crowd. Theoretical analysis and simulations showed that SACRM can productively improve the crowdsourcing utility and can enhance the quality of their sensing reports.

Further, S. Joshi et al. [10] had planned different figures and key information for shaping trust like Ant Based Evidence Distribution (ABED), Generalized Reputation evidence (GRE), Secure and Objective Reputation based Incentive (SORI) and so on. They have proposed some trust based plans that were talked about for the trust foundation in MANET (Mobile Ad Hoc Network) like Protocol Based Trust Scheme, System Based Trust Scheme, Cluster Based Trust Scheme, Maturity Based Trust Scheme, and PKI Based Trust Scheme. Even though the researchers never ensured that this work can be implemented in real but their work proposed huge discoveries towards trust.

Table 2.1 Techniques/Parameters proposed by various scientists/researchers

Authors	Parameters	Technique Used
H. Lin et al. [6]	Mean Standard Deviation and Standard Error.	Wisdom Of Crowd
A. C. Weaver et al. [7]	1. Reliable User 2. Average ranking and Number of users. 3. GPS coordinates and IMEI (International Mobile Equipment Identity) numbers.	Three Schemes 1. Trust Associated with Group Membership 2. Trust Determined by Crowdsourcing 3. Trust Determined by Machine Learning (Game Theory, Machine Learning algorithm “neural network algorithm” and Data Mining)
Y. Liu et al.	Accumulative regret,	Online algorithm LS_OL

[8]	Average regret, Time steps, Average error rate, Accumulative rewards, Average Rewards, Number of disagreement, Ordered image number, CDF (cumulative distribution function) and Error in labeling	
J. Ren et al. [9]	Time complexity, Space complexity, Random distribution (RD), Normal distribution (ND, Utility, Task Budget, Actual Delay, Number of Mobile users, Rewards, Veracity Scores, Reputation Value, Report quality and Bid Price	SACRM: Social Aware Crowdsourcing with Reputation Management
S. Joshi et al. [10]	Reliability Index, Node cooperation Index, Trust Factor and disjunction of selfish index.	Mobile Ad Hoc Network (MANET)

Mobile crowd sourcing is an agile technology looking for continuous upgrades these upgrades are an effort to make crowdsourcing more effective than before.

Czerwinski et al. [11] made it possible to use Service Discovery Service (SDS). Complex description of already running services was promoted by the service providers using SDS, while clients were using SDS for making interconnected research for finding these services. It is very convenient to use SDS as a service. SDS adapts to overcome the failures of the dual SDS servers and the services. It hides the complex fault recovery method from the customer's application. SDS ensures safe and secure interaction between the components of the system. Extensible Markup Language (XML) is used by service description and questions to encode factors like cost, execution, area and gadget. SDS enables the services to grab sensitive data and helps find useful services to the clients.

Priyantha et al. [12] developed a compass that was so compact that it could be integrated in a handheld mobile device. This was known as "Cricket Compass". It was used to locate and determine the orientation of the mobile device it was mounted on. The system worked based on an application the mobile device which received the position and orientation in a local coordinate system which was predetermined by a fixed group of beacons. This comprised of 5 ultrasonic receivers with a diameter of 0.8cm which was kept in a formation of "V" shape placed a few centimeters apart. When installed in a building this system computed 418 MHz RF data and 40 KHz ultrasonic signals were produced by the beacons. The result of this test was that the compass could locate and find the orientation within 3 degrees for the actual value which is 30 degrees.

Sastry et al. [13] solved the problem of location verification by coming up with a protocol known as the Echo Protocol. This method was a very primitive way of secure location verification. It was ultra-lightweight but the most impressive feature of this protocol is that it does not require time synchronization and cryptography. The protocol proved its worth when 80-90% of the locations claimed that the protocol ensured in region verification.

Zhang et al. [14] proposed a direct method in which with the help of transmitters challenges were send that were witnessed by the nodes that were claiming for the location and challenges were also based on that claimed location furthermore the claiming node should properly response to the challenge to prove that its claim is true. Then after direct method and indirect method comes into role where the transmitter again sends the challenges but this time claiming node cannot witness those challenges. Finally, a signal based method is introduced in which response by nodes are given with the signal strength that is received and thus it location verification is also improved. For the evaluation of the scheme researchers had examined different adversarial models. Under these adversarial models the performances of power-modulated challenge scheme were defined. Result demonstrated the performance against a smart adversary was worse than the performance against naive adversary.

Saroiu et al. [15] proposed 6 applications which functioned based on infra providing location proofs. A stable protocol was put forward which could be implemented over a Wi-Fi network where location proofs to the mobile devices were provided by APs. Mobile applications made use of this protocol which enabled them to share their past and present locations.

Gilber et al. [16] put forward a dependable sensing protocol to safeguard the privacy of the participants. This protocol could be used on mobile devices featuring TPM hardware and enabled with access control policies as well has explicit user authorization. Because of the highly authentic data and increased level of privacy this platform was supposed to elevate the value of service providers and the owners of the device.

Saroiu et al. [17] enabled mobile devices to authorize applications by including trusted sensors on the device. It also presented 2 different designs to identify sensor readings as ‘trusted’. The first was a TPM based design which relied on a virtualized environment to provide trusted sensor readings. Second was a design that merged trusted computing primitives right on to the sensors. In the end the privacy issues that came forward because of the use of trusted sensorswere analyzed. The outcome showed how anonymous credential schemes, zero knowledge protocols, and witness-hiding protocols can control these privacy issues. Design # 1was less secure to hardware attacks than the Design # 2.

Amintoosi et al. [18] put forward an application agnostic trust framework for social participatory sensing system. Trustworthiness of the participants and the quality of data are separately calculated by this system. Then a fuzzy logic engine is used to combine the quality and trustworthiness to compute the trust ranking for every individual contribution. A large scale simulation was conducted to portray the efficiency of the system. A hike of 15% was observed in overall trust as a result of the simulation.

Luo et al. [19] proposed different algorithms like Simple Endorsement Web (SEW), Nepotism a social concept was also introduced into participatory sensing. This was done with endorsement relations in which linking of mobile users into a social “web of participants” were done. Economic implications were used as investment to cover web of participant’s network. Stackelberg game framework was used to analyze economic implications and even the social implication were also extended. For increasing the utility of sensing campaign organizer an optimal design parameter was developed. Finally for the manipulation of endorsement links an algorithm was designed. Talking about the results Nepotism turned out to be a strong source for motivating trustworthy crowd sourcing and even the two elements namely social and Economic were also connected.

C. Wu et al. [20] invented an endorsement-based reputation system for evaluating the trust of workers. This system is unique as it takes endorsement of other workers into account. In this system first of all an endorsement network was made to exhibit the endorsement correlation between the workers. Then to estimate the reputation of a worker the assessor will take into account the workers it endorsed to evaluate the target worker’s competence by ranking collaborative filtering. Feedback of the workers was then used to assess the trust evaluation result. With the expertise taken into account the reputation of the target worker is assessed.

Table 2.2 depicted some recent papers that highlight the objectives, techniques, advantages and disadvantages and scope of improvement in future directions.

Table 2.2 Number of approaches proposed by various scientists/researchers

Ref No.	Objective	Method Used	Advantages	Disadvantages
Czerwinski et al. [11]	To design secure and trusted environment.	Service Discovery Service (SDS).	It helps to create secure communication between components and ensures the trustworthiness.	Does not deal with real services and clients applications.
Priyantha et al. [12]	To develop a compact Compass that could be integrated in a handheld mobile device.	Cricket Compass.	It helps to localize the devices.	Security is not taken care of as GPS signals can be spoofed easily.
Sastry et al. [13]	To develop some protocols	Echo Protocol.	Solved the problem of location verification and	This verification of location claim can lead to the problem of

	for location confirmation.		can be used for location-based access control.	authentication.
Zhang et al. [14]	To verify the location.	Direct and Indirect methods for transmitting the challenges.	Gives authentication to the task by proving the position of the entity.	This technique can also be used for users to certify their location proofs to mobile applications so that their privacy properties can be enhanced.
Saroiu et al. [15]	To enable users to proof their location.	Location proofs.	Helped mobile devices to securely proof their current and past position.	Witnesses are only limited to areas where infrastructure has already been deployed and it is not important that data altered is fully assured it may be possible that pre-manipulated data is submitted for signing.
Gilber et al. [16]	To build a trustful platform.	Trusted Platform Module	They have built a trusted	The sensors are trusted but security and

		(TPM) hardware.	platform model for both service provider and mobile users.	privacy properties are very week.
Saroiu et al. [17]	To identify sensor readings as ‘trusted’.	TPM based design which depends upon virtualized environment. Second design was sensors merged with trusted computing primitives.	Many applications were benefited by TPM and properties like security and privacy were strongly achieved.	They are yet to be adopted widely in mobile devices.
Amintoosi et al. [18]	To design a framework for social participatory sensing system.	Fuzzy trust framework.	It motivates the large group of mobile users to participate and ensures that the data that is sensed is trust worthy.	Participants are treated individually.
Luo et al. [19]	To motivate large grou	Nepotism a social concept, Simple	It not only motivates and ensures trust	It just surveys information quality after

	p of people to participate and to ensure tha t the sensing data is trusted.	Endorsement Web (SEW) algorithm.	but in this there is relationship among the participants’. (Social and economic)	receivingvthe contributions, which results in workers paying unnecessary irreversible efforts.
C. Wu et al. [20]	To evalua te the trust of workers.	EndorTrust, endorsement-based reputa tion system.	It evaluates the trust of workers, by taking the endorsement ofother workers into account.	It supports Medium level Worker Trust (WT) and Data Trust (DT). Which means Collusion and False data Uploading is not taken into consideration.

2.2 PRIVACY ISSUE

Mobile crowdsourcing is an advancing field of study that invites number of drawbacks and challenges. This section deals with mobile crowdsourcing and also with one of its most important issues i.e. Privacy Issue. Numbers of scientists/researchers have proposed several privacy techniques for mobile crowd sourcing.

Y. Gong et al. [21] defined trade-off among three factors i.e. utility, privacy, and efficiency. They characterized task selection as NP-hard proble and then proposed an approximation algorithm and privacy-preserving protocol for its solution.

Later in Y. Gong et al. [22] researcher resolved the problem of worker feedback that was required in their approximation algorithm by efficient aggregation approach.

R. Liu et al. [23] set up a system known as PriWe. This system was deployed so that user's prospect about privacy is known and accordingly recommendations were made for privacy settings of the mobile apps that users have installed. For comparing the success rate of PriWe, task was published on Amazon Mechanical Turk and PriWe itself was executed in real world. The feedback from Amazon Mechanical Turk by 382 participants showed that PriWe achieved 78% accuracy when all participants are taken into consideration and 90% accuracy was achieved when people with the background of privacy and security were taken, and from real world 78 users recommended PriWe as a proper method to meet the privacy expectation of mobile users

C. M. Tseng et al. [24] had discussed a solution for the privacy of the sensing data of the vehicles that was crowd sourced. The solution was type-revealing privacy enhancing mechanism based on Laplacian mechanism. To be more précised we can say that author proposed the solution for the privacy of crowd-sourced data in transportation applications like eco-routing and DTE (Distance-to-empty) prediction.

Y. Wang et al. [25] proposed an incentive mechanism which further included two algorithms which were ITA (Improved Two-stage Auction) and TORU (Truthful Online Reputation Updating). This mechanism joined the advantages of both online and offline mechanism and then statically selected a worker further after biding it even selected the winner.

B. Zhang et al. [26] proposed a participant coordination framework, in which without knowing the participants trajectories an optimal QoI was provided for task sensing. Further for the participants privacy data aggregation, incentive distribution method and punishment method was proposed.

T. Kandappu et al. [27] showed specific threats due to continuous sharing of location and also showed that for location privacy a simple trajectory obfuscation technique could be used.

J. H. Ziegeldorf et al. [28] introduced TraceMixer for achieving privacy and data utility of crowd sensing. TraceMixer was based on the concept of mix zones to provide trajectory privacy.

L. L. Zhang et al. [29] build risk rating a way to communicate risks of privacy for app-specific. This concept was enforced for application distribution providers (e.g., Microsoft, Apple, and Google) in Privet, system.

Table 2.3 Techniques/Parameters proposed by various scientists/researchers

Authors	Parameters	Technique Used
Y. Gong et al. [21]	Revenue, Utility and Computation overhead.	Recommendation system, Greedy algorithm and Privacy-Preserving Aggregation Protocol
Y. Gong et al. [22]	Average Revenue, Number of recommended task, Weighted Sum of Utility and Efficiency and Computation overhead.	Recommendation system, Greedy algorithm and Efficient aggregation approach.
R. Liu et al. [23]	Accuracy and Number of users	PriWe
C. M. Tseng et al.	Estimation error and Energy Estimation	Type-revealing privacy enhancing mechanism

[24]	error.	
Y. Wang et al. [25]	Auction efficiencies and Transaction time	Incentive mechanism including two algorithms: 1. Improved two-stage auction algorithm (ITA) 2. Truthful online reputation updating algorithm (TORU)
B. Zhang et al. [26]	Average number of instance and Reduction in time	Participant coordination framework
T. Kandappu et al. [27]	Efficiency and Entropy gain	Simple Trajectory Obfuscation
J. H. Ziegeldorf et al. [28]	Runtime, Average time span and Tracked distance	TraceMixer
L. L. Zhang et al. [29]	Incentive Budget, Selected participants and Redundant Data	Risk Rating

Mobile crowdsourcing as a technology is gaining momentum in real world scenario. With this real world implementation the ability of a technology to keep itself updated with requirements of the time is needed that makes the technology more dependable and effective than before.

A.C. Myers et al. [30] proposed a label model so that it was possible to control information flow so that privacy was achieved. It was not accepted by everyone due to the restrictions it imposed and it also had computational overhead. Another thing that the author mentions in the paper was programming language known as Jif. Jif permitted the static checking of information flow.

W. Enck et al. [31] proposed a solution for mobile phones operating system known as TaintDroid. TaintDroid made mobile phone users aware about how their personal data was used by third-party applications. TaintDroid was implemented over 30 popular third-party applications and the results clearly showed that in 20 applications there were 68 instances where user's personal information was misused.

A.R. Beresford et al. [32] proposed MockDroid, which we can say was the improved version of TaintDroid as it also helped user to identify the applications that are misusing their personal data in addition it also helped the users to mock their identity in such case.

J. Lin et al. [33] introduced a model named Privacy as Expectations. As the name clearly indicates it insured the privacy of personal data according to the user's expectations. Author not only achieved the privacy according to the users wish but also showed the impact on users feeling and trust decisions when their private data is misused. Author also suggested that by informing the users about why and how is their personal information is used will also reduce the great concern of privacy.

Y. Agarwal et al. [34] proposed ProtectMyPrivacy (PMP), for the iOS devices which identified the applications using the personal data and helped the user to send false information if they wish to, thus protected their information.

X. Chen et al. [35] presented PMG (Privacy Preserving Map Generation). PMG was to protect the private information of user that was his/her location. In it the location of the user was randomly placed so that it was difficult to trace the original location.

Y. Yao et al. [36] proposed a protocol so that three major factors could be achieved like protecting privacy, accuracy of data and generality. The protocol was named as efficient anonymous data reporting protocol. This protocol consisted of two stages that were slot reservation and message submission. These two stages broke the link between the user and user personal data, thus helping in protecting the privacy of the user as the user could not be identified without the personal information.

S. Gisdakis et al. [37] proposed architecture for Mobile Crowdsourcing that was novel secure and accountable to achieve security, privacy and resilience.

Table 2.4 contains researches which had some limitations and were used as a scope of improvement in the next research.

Table 2.4 Number of approaches proposed by various scientists/researchers

Ref No .	Objective	Method Used	Advantages	Disadvantages
Myers et al. [30]	To contro l the informatio n flow in system s.	Decentralized label model	Privacy in a complex and decentralized w orld, Jif was proposed to ensure the compiler security.	These languages require accurate development and are incompatible with software designs.
W. Enck et al. [31]	To propose solutions for Smartpho ne so that users are aware about ho w the third party applicatio	TaintDroid	TaintDroid improved the effectiveness of Smart phones.	Conditions like false negative and false positive was experienced by this system and it could only identify the information being violated but could not take any measures to

	ns are using their personal data.			protect it.
A.R. Beresford et al. [32]	To aware the users about how their privacy is being misused and further securing the privacy.	MockDroid	Allowed user to ‘mock’ by reporting the resource as empty or unavailable to the applications	Could not identifyvuser’s point of view regarding if the action taken was reasonable or not.
J. Lin et al. [33]	To know users perspective about what permission they want to grant to a particular application.	Privacy as Expectations model	Privacy concerns of users were satisfied to some extend as users were notified properly about the usage.	Users were notified about the privacy after installation.
Y.	To	ProtectMyPri	Sending	Authenticity of

Agarwal et al. [34]	achieve privacy of users in iOS devices.	vacy (PMP)	false data helped in achieving privacy e.g. sending fake location	data was compromised and some services were also damaged.
X. Chen et al. [35]	To hide users location.	Privacy Preserving map generation scheme	Privacy demands of users were achieved.	There was no generality and therefore was applicable for only some applications.
Y. Yao et al. [36]	To secure the private data.	Data reporting protocol (broke down the link between data and the participants)	Privacy was preserved as there was no connection between data and user.	There was no framework to tackle the misbehavior of users.
S. Gisdakis et al. [37]	To hide users identity.	A novel secure and accountable MCS Architecture for user's personal information management	Through this management scheme the identity of the user was well protected	Only the identity of the user was protected but data privacy was not fully achieved.

CHAPTER 3
PROBLEM DESCRIPTION

OBJECTIVE: To solve the issue of trust and privacy in mobile crowdsourcing.

There are three main issues in crowdsourcing.

- **Security**
- **Privacy**
- **Trust**

Security Issue occurs between the User and the Service Provider. In this it may be possible that the user that is asking for services is not an authorized user or we can say is just an attacker who may misuse the information provided by the service provider.

Privacy Issue occurs between the Service Provider and the particular Application which is providing the data. In this the issue arises when the personal details of an individual are also revealed as the personal details may be misused.

Trust Issue occurs between the Particular Application and the workers or the employees that are providing the information to the application. The issue is that is the information that is provided by the employee or the worker is valid or not.

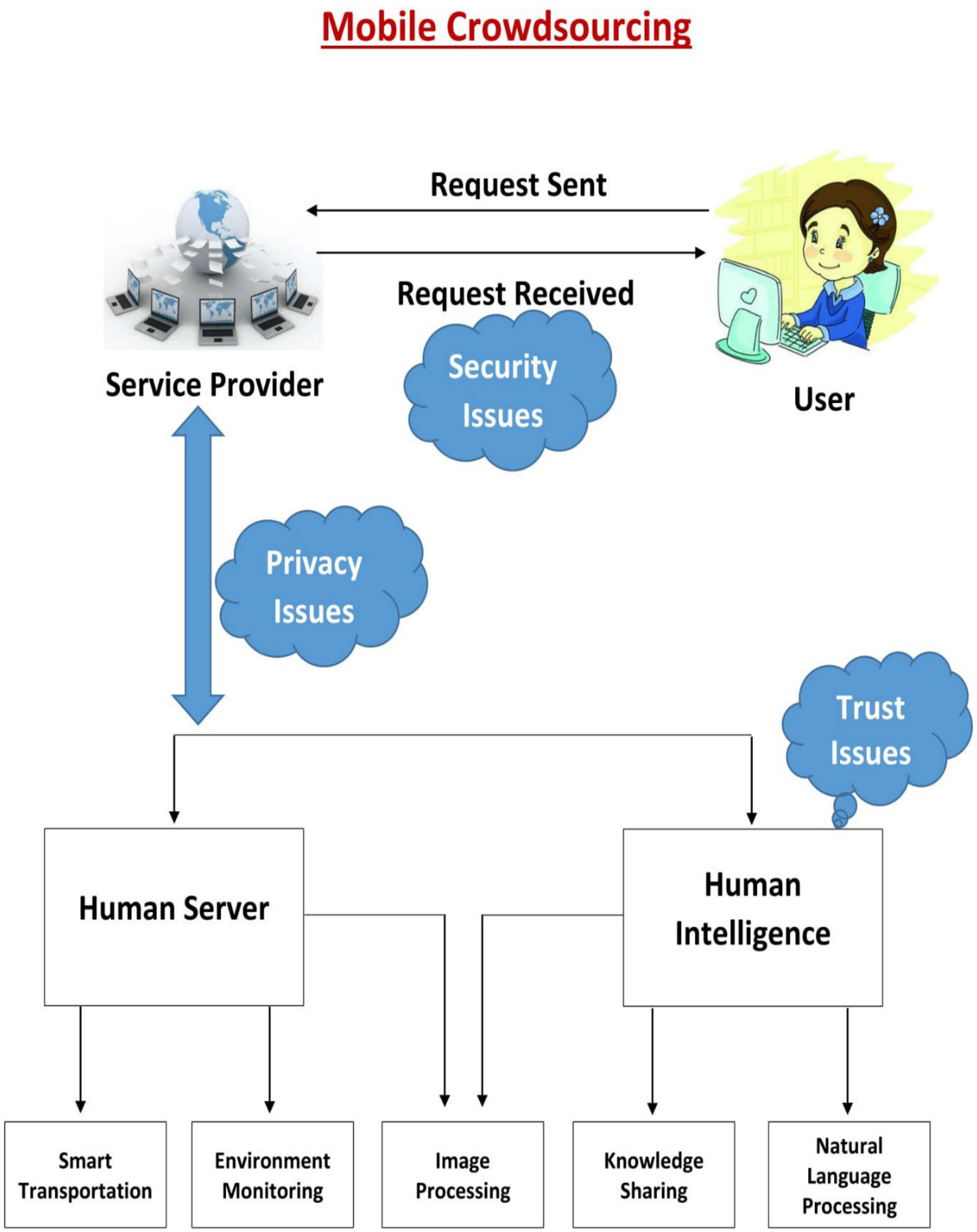


Figure 3.1 Mobile Crowdsourcing Issues

CHAPTER 4

PROPOSED SOLUTION

4.1 TRUST ISSUE

In this paper, we have used Dempster–Shafer Theory (DST) to evaluate trust during the data gathering and transmission among mobile users. DST also known as theory of belief function originated from the work of Arthur P. Dempster. However, theory was later developed by Glenn Shafer known as a mathematical theory of evidence (Theory of evidence) so that the uncertainty could be modeled [38]. In mathematics DST framework is a framework in which evidence from different sources was combined and under uncertainty a degree of belief was reached from the range [0, 1] and the reputation of ignorance was lowered [39]. The step-wise description of the DST is briefed in the below text.

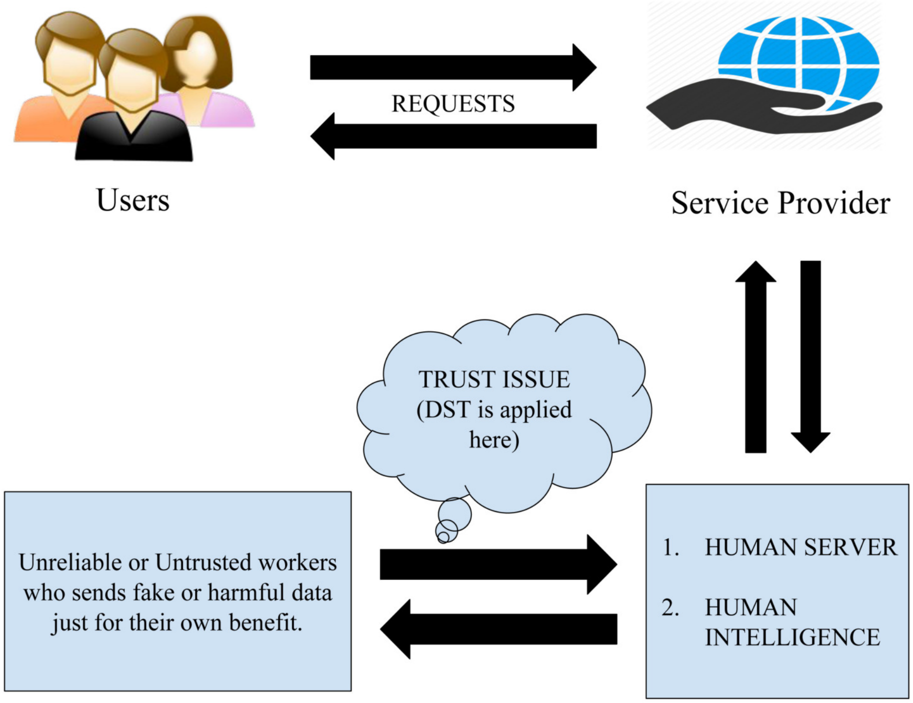

REQUESTS
Users
Service Provider
TRUST ISSUE (DST is applied here)
Unreliable or Untrusted workers who sends fake or harmful data just for their own benefit.
1. HUMAN SERVER
2. HUMAN INTELLIGENCE

Figure 4.1 Using DST in Mobile Crowdsourcing Model

Step 1: Let S be the finite set of system propositions, and its power set is$P = 2^{\theta}$.

We define a basic beliefvassignment (BBA) as a function m: P → [0, 1] such that it satisfy following two conditions

1. $\boldsymbol{M\{\phi\} = 0}$;
2. $\boldsymbol{\sum_{A \epsilon P} m(A) = 1}$.

Let's say for a binary case we have m ({x} + m{y} + m{x, y}) =1.

$$m(x \cup y) = m(x) + m(y) - m(x \cap y)$$

$$m(x \cup y \cup z) = m(x) + m(y) + m(z) - m(x \cap y) - m(x \cap z) - m(y \cap z) - m(x \cap y \cap z)$$

Where $m(x \cap y) = m(x) * m(y)$ and $m\{x, y\} \rightarrow m(x \cup y)$

Each hypothesis A ∈ P has two bounds; lower which is called belief (Bel) and upper which is called plausibility (Pl).

Step 2: The belief in an element A of the Power set is the sum of the masses of elements which are subsets of A (including A itself).

$$\boldsymbol{Bel(A) = \sum_{B|B \subseteq A} m(B).}$$

Let's say for a binary case we have

Bel ({x}) = m ({x});

Bel ({y}) = m ({y});

Bel ({x, y}) = m ({x}) +m ({y}) + m ({x, y}).

Step 3: The plausibility of an element A, pl (A), is the sum of all the masses of the sets that intersect with the set A.

$$\boldsymbol{PI(A) = \sum_{B|B \cap A = \emptyset} m(B).}$$

Let's say for a binary case we have

PI ({x}) = m ({x}) + m ({x, y});

PI ({y}) = m ({y}) + m ({x, y});

PI ({x, y}) = m ({x}) +m ({y}) + m ({x, y}).

Step4: Belief intervals allow Dempster-Shafer theory to reason about the degree of certainty or uncertainty of our beliefs.

$$\boldsymbol{BI(A) = PI(A) - Bel(A)}.$$

- A small difference between belief and plausibility shows that we are certain about our belief.
- A large difference shows that we are uncertain about our belief.
- However, even with a 0 interval, this does not mean we know which conclusion is right.

  Let's say for a binary case we have

  BI ({x}) = PI ({x}) - Bel ({x});

  BI ({y}) = PI ({y}) - Bel ({y});

  BI ({x, y}) = PI ({x, y}) - Bel ({x, y}).

4.2 PRIVACY ISSUE

The solution proposed to protect the privacy of the users is the combination of Advanced Encryption Standard (AES) and SALT cryptography. Advanced Encryption Standard (AES) is a process to convert raw information i.e. plaintext into a form which is not readable and a key is generated along it only through that key decryption is possible. Cryptography means that the message transmitted is in such a form that only receiver can decode it, the plain text is changed to cipher text and only the authenticated receiver can transform it to original text [5]. SALT is random data that is added to any other data before hashing of data is done and thus increasing the effort of reversing the data. Therefore this combination is used for preserving the privacy of the hashed data from the attacks like brute force, rainbow table and dictionary attack. The unique quality of SALT is that it can be different for different users not like hash function [5].

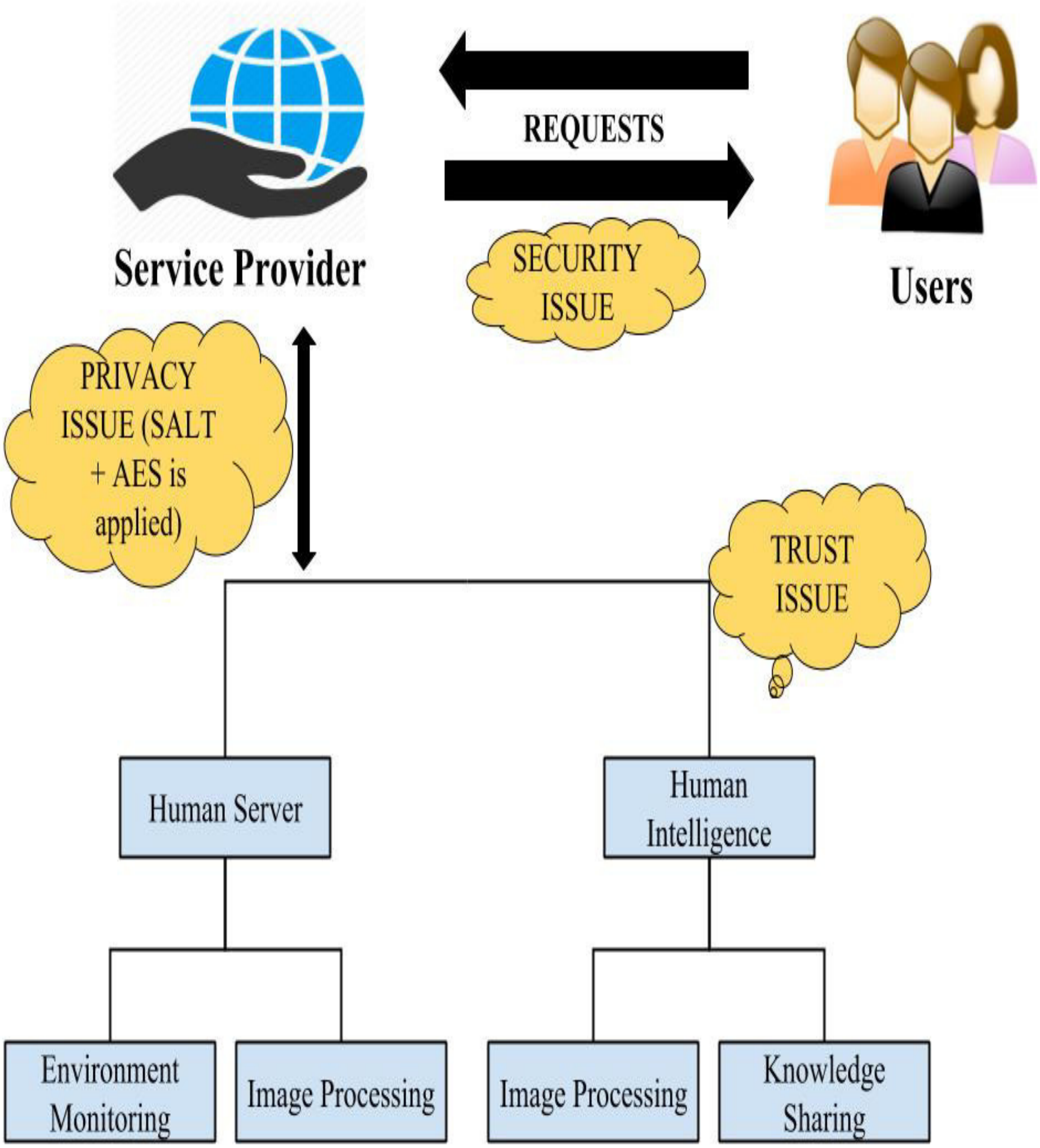


Figure 4.2 Using (SALT + AES) in Mobile Crowdsourcing Model

CHAPTER 5
PROPOSED ALGORITHM

5.1 TRUST ISSUE

In this paper, we have used this phenomenon in whichvwith the group of n number of peoples and n number of products we have n number of Ratings of products $(RT1, RT2\ldots RTn)$. Further, we divide the Rating of n users into different types than the new set is defined as:

Poor (Rating of product i.e. 1 and 2(RT1))

Moderate (Ratingvof product i.e.3 (RT2))

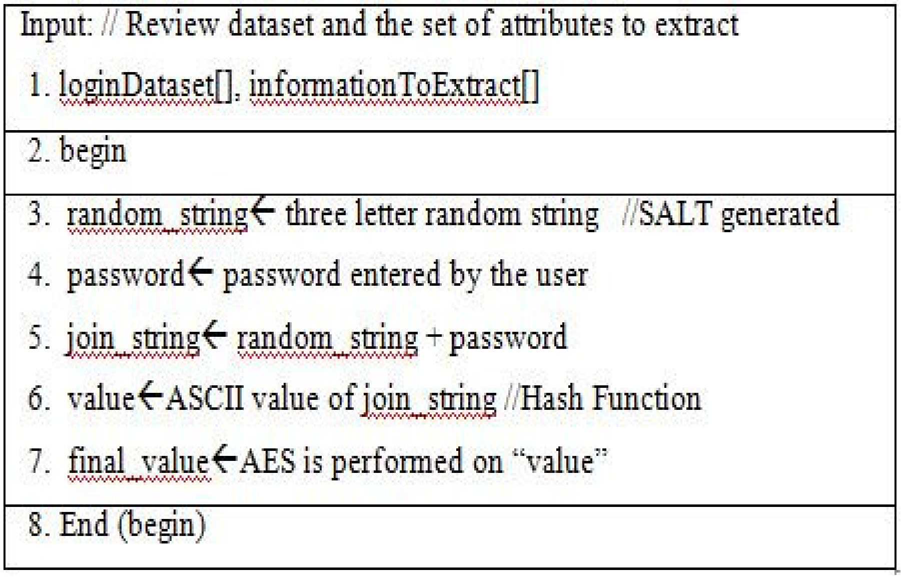
Good (Rating of product i.e. 4 and 5 (RT3))

(RT1, RT2, RT3, RT4, RT5, RT6, RT7, PD1)

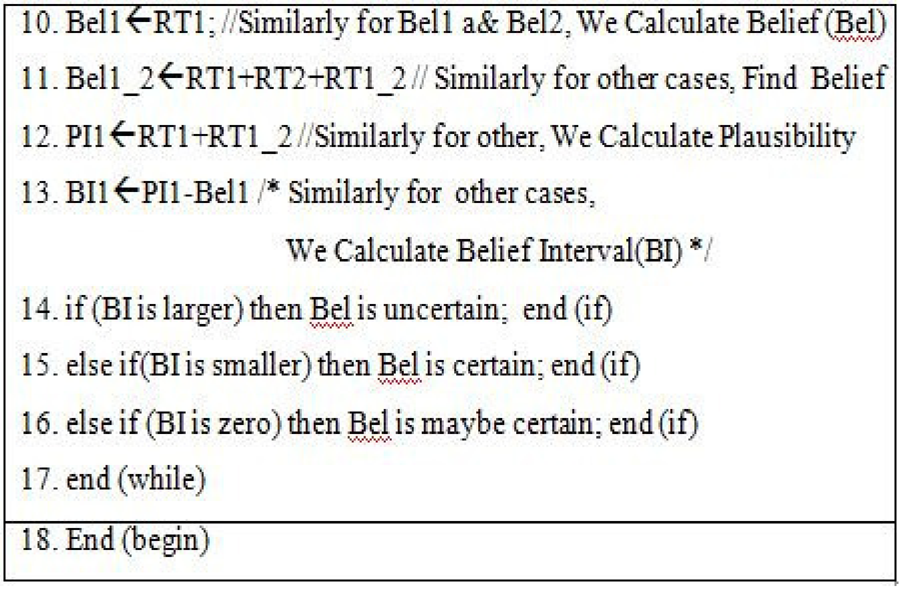
Here RT1, RT2, RT3, RT6…. are the ratings of different users on similar product.

PD1,vPD2 are different products. Table 5.1 depicts the algorithm of Dempster-Shafer Theory used to evaluate the trust among mobile users.

Table 5.1 Algorithm for Trust Issue



```
Input: // Review dataset and the set of attributes to extract
 1. loginDataset[], informationToExtract[]
 2. begin
 3. random_string← three letter random string   //SALT generated
 4. password← password entered by the user
 5. join_string← random_string + password
 6. value←ASCII value of join_string //Hash Function
 7. final_value←AES is performed on "value"
 8. End (begin)
```

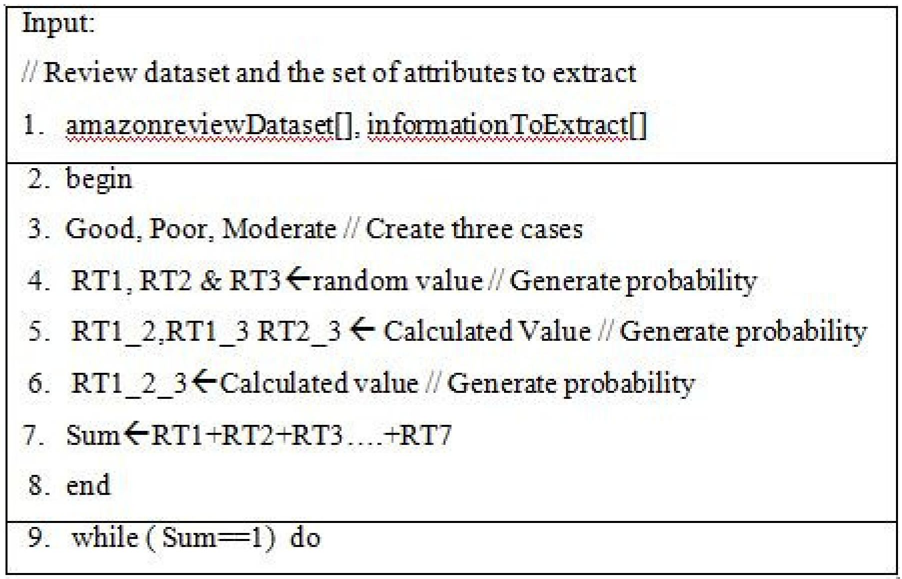


```
Bel1←RT1; //Similarly for Bel1 a& Bel2, We Calculate Belief (Bel)
Bel1_2←RT1+RT2+RT1_2 // Similarly for other cases, Find  Belief
PI1←RT1+RT1_2 //Similarly for other, We Calculate Plausibility
BI1←PI1-Bel1 /* Similarly for  other cases,
                    We Calculate Belief Interval(BI) */
if (BI is larger) then Bel is uncertain;  end (if)
else if(BI is smaller) then Bel is certain; end (if)
else if (BI is zero) then Bel is maybe certain; end (if)
end (while)
End (begin)
```

5.2 PRIVACY ISSUE

Three random letters are added as SALT to the data. Then for hashing purpose ASCII value of each letter of data is generated. Then on this hashed function Advanced Encryption Standard (AES) is performed. SALT is only stored in the database if desired by the user.

Table 5.2 Algorithm for Privacy Issue



```
Input:
// Review dataset and the set of attributes to extract
amazonreviewDataset[], informationToExtract[]
begin
Good, Poor, Moderate // Create three cases
RT1, RT2 & RT3←random value // Generate probability
RT1_2,RT1_3 RT2_3 ← Calculated Value // Generate probability
RT1_2_3←Calculated value // Generate probability
Sum←RT1+RT2+RT3….+RT7
end
while ( Sum==1)  do
```

CHAPTER 6
EXPERIMENTAL SETUP

6.1 TRUST ISSUE

In order to conduct the experiment we collected freely available data of 1500 customer regarding Amazon product reviews. Out of these 1500 we selected a sample of 103 entries. This data consisted of Product I.D, Product Name, Rating, Review Text, User Name etc. These 103 samples consisted of 4 products from which 1 product was selected at a time so as to enable our algorithm to be applied on it. The rating of customers that were 1 -5 were divided and categorized into three cases. Further the probability was calculated for all the three categories and if the sum of these probabilities were 1 then the algorithm continued or else the probability was calculated again. If the algorithm continued it would calculate 'belief' i.e. an acceptance that something is true. After this the algorithm further calculated 'plausibility' i.e. the degree of probability of something being true. Then 'Belief Interval' i.e. difference between plausibility and belief was calculated. If the difference came out to be large then the belief was 'uncertain', if the difference came out to be small the belief was 'certain' and if the difference came out to be zero the belief 'maybe certain'.

6.2 PRIVACY ISSUE

For experimental purpose we took the Captive portal Login details of 30 students of our university (Jaypee University). The dataset was collection of Roll No., Login ID, and Password. Three letter SALT was generated randomly and then was added to the password the new password so formed after addition of SALT was then hashed, for hashing purpose the letters of new password was converted to their ASCII values and then

AES was applied on that hashed value which was then stored in the form of password in the data set. For showing the results the text or the password taken was:

- t1: “hellohello”,
- t2: “hellohellohellohello”,
- t3: “hellohellohellohellohellohello” and
- t4: “hellohellohellohellohellohellohellohello”

Further these texts were compared with normal AES and DES.

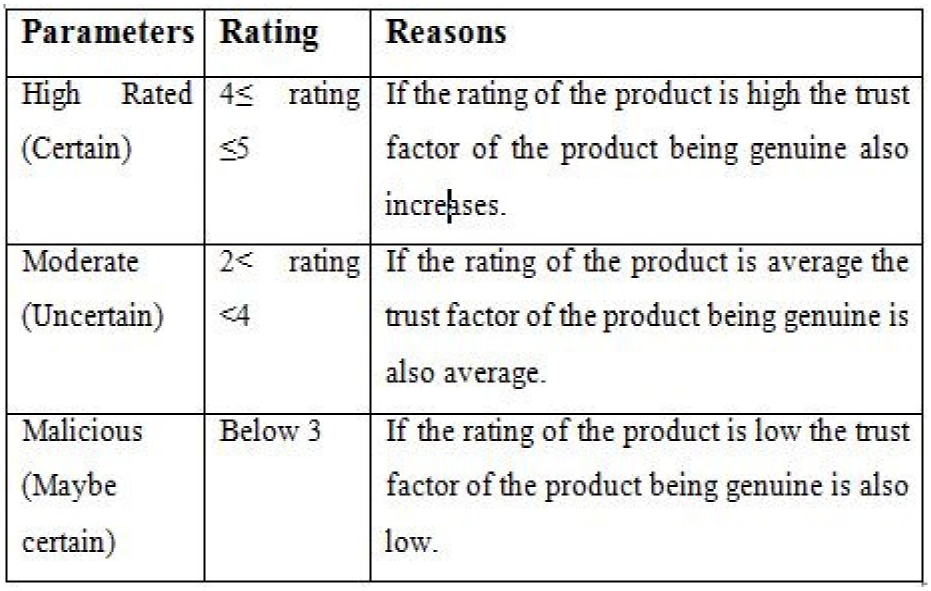
CHAPTER 7

EXPERIMENTAL RESULTS AND ANALYSIS

7.1 TRUST ISSUE

The performance matrices shown in table 7.1 are used to compute or to measure the performance of the proposed algorithm.

Table 7.1 Performance Parameters for DST (Dempster–Shafer Theory)



Parameters	Rating	Reasons
High Rated (Certain)	4≤ rating ≤5	If the rating of the product is high the trust factor of the product being genuine also increases.
Moderate (Uncertain)	2< rating <4	If the rating of the product is average the trust factor of the product being genuine is also average.
Malicious (Maybe certain)	Below 3	If the rating of the product is low the trust factor of the product being genuine is also low.

The users who rated the product 1or 2 were categorized as poor, users who rated the product 3 were of moderate quality and the users who rated the product 4 or 5 were kept in good category. Based on this divisionvseven probabilities of overall product quality were taken into account such as:

1) Poor,

2) Below Average (Poor Union Moderate),

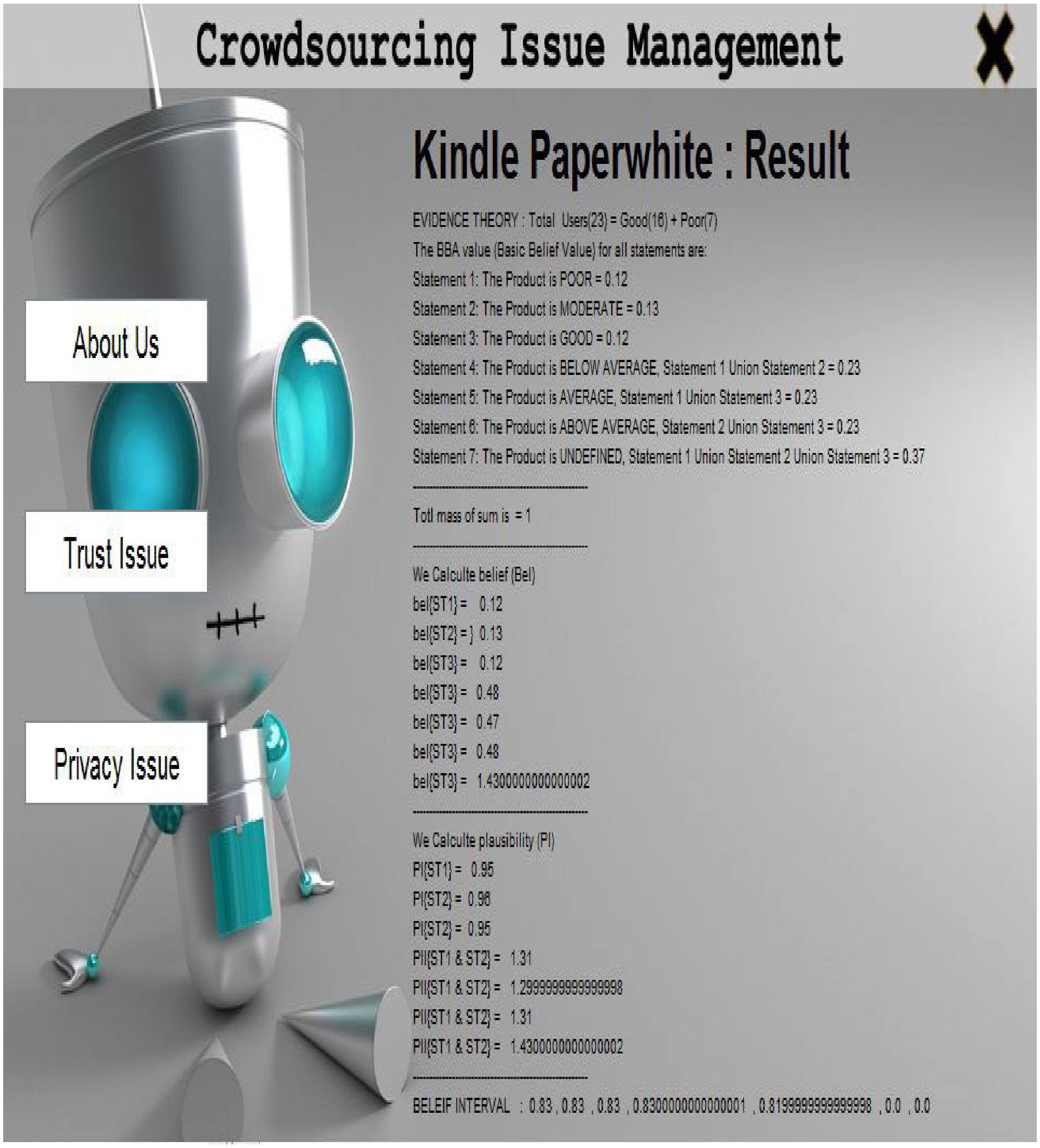
3) Moderate,

4) Above Average (Moderate Union Good),

5) Good,

6) Average (Poor Union Good), and

7) Undefined (Poor Union Moderate Union Good).



```
EVIDENCE THEORY : Total  Users(23) = Good(16) + Poor(7)
The BBA value (Basic Belief Value) for all statements are:
Statement 1: The Product is POOR = 0.12
Statement 2: The Product is MODERATE = 0.13
Statement 3: The Product is GOOD = 0.12
Statement 4: The Product is BELOW AVERAGE, Statement 1 Union Statement 2 = 0.23
Statement 5: The Product is AVERAGE, Statement 1 Union Statement 3 = 0.23
Statement 6: The Product is ABOVE AVERAGE, Statement 2 Union Statement 3 = 0.23
Statement 7: The Product is UNDEFINED, Statement 1 Union Statement 2 Union Statement 3 = 0.37
--------------------------------------------
Totl mass of sum is  = 1
--------------------------------------------
We Calculte belief (Bel)
bel{ST1} =    0.12
bel{ST2} = } 0.13
bel{ST3} =    0.12
bel{ST3} =  0.48
bel{ST3} =  0.47
bel{ST3} =  0.48
bel{ST3} =  1.4300000000000002
--------------------------------------------
We Calculte plausibility (Pl)
Pl{ST1} =  0.95
Pl{ST2} = 0.96
Pl{ST2} = 0.95
Pll{ST1 & ST2} =  1.31
Pll{ST1 & ST2} =  1.2999999999999998
Pll{ST1 & ST2} =  1.31
Pll{ST1 & ST2} =  1.4300000000000002
--------------------------------------------
BELEIF INTERVAL  : 0.83 , 0.83  , 0.83  , 0.8300000000000001  , 0.8199999999999998  , 0.0  , 0.0
```

Figure 7.1 Results when DST is applied

In the above figure we can see that the Belief interval for average was minimum i.e. 0.8199 than the possibility of the product being “Average Quality” is more than others.

7.2 PRIVACY ISSUE

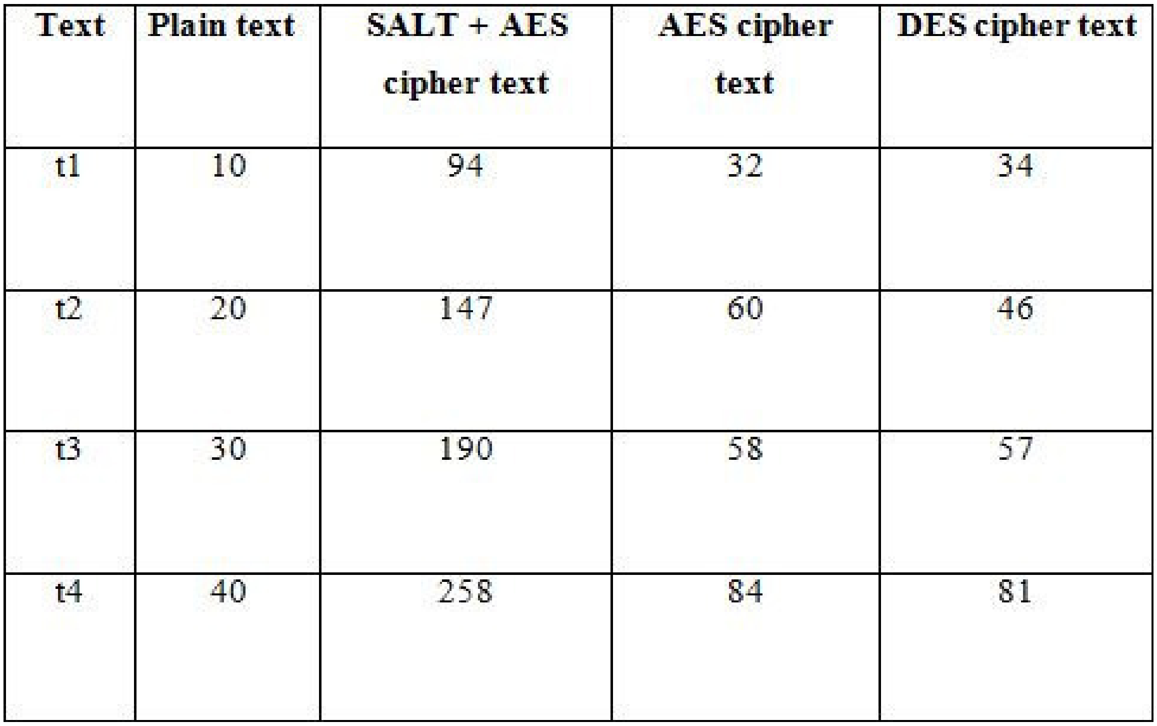
Advanced Encryption Standard (AES) is a process to convert raw information i.e. plaintext into a form which is not readable and a key is generated along it only through that key decryption is possible.

Data Encryption Standard (DES) is a method to convert plaintext to ciphervtext usingvsingle keyvfor both encryption and decryption.

1. **Plain text size vs. Cipher text size**, size of text plays an important role in cryptography as the size of text is big more effort are required to crack it [40]. Table 7.2 and Figure 7.2 show the comparison between the cipher text size among SALT + AES cipher, AES cipher and DES cipher.

   The resultvclearly shows that the cipher text size of SALT + AES cryptographyvwas greater than others.

Table 7.2 Comparison of Text size (in bytes)



Text	Plain text	SALT + AES cipher text	AES cipher text	DES cipher text
t1	10	94	32	34
t2	20	147	60	46
t3	30	190	58	57
t4	40	258	84	81

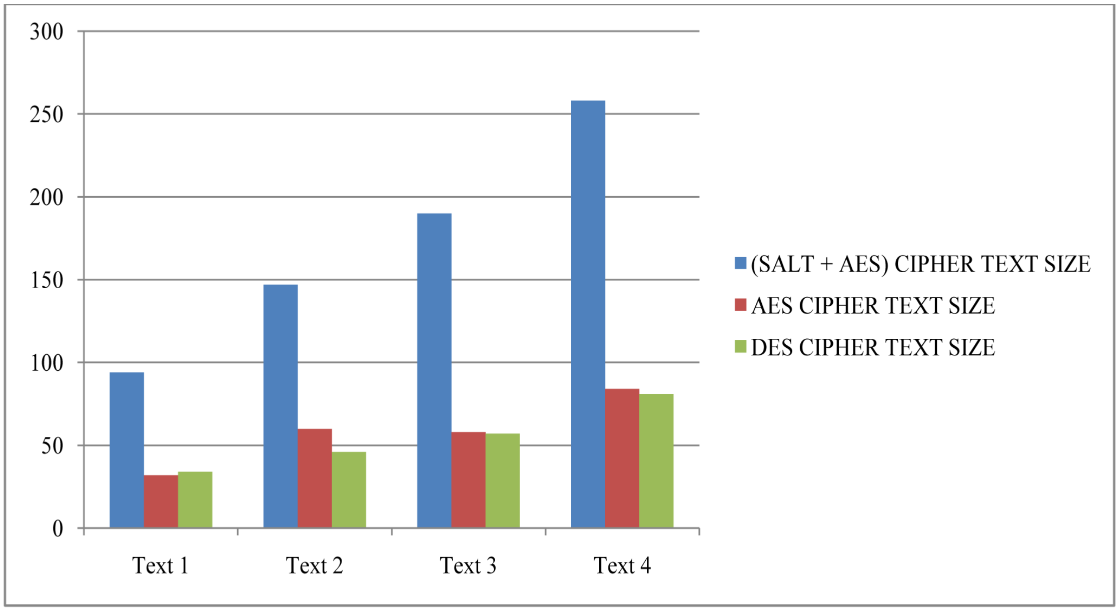
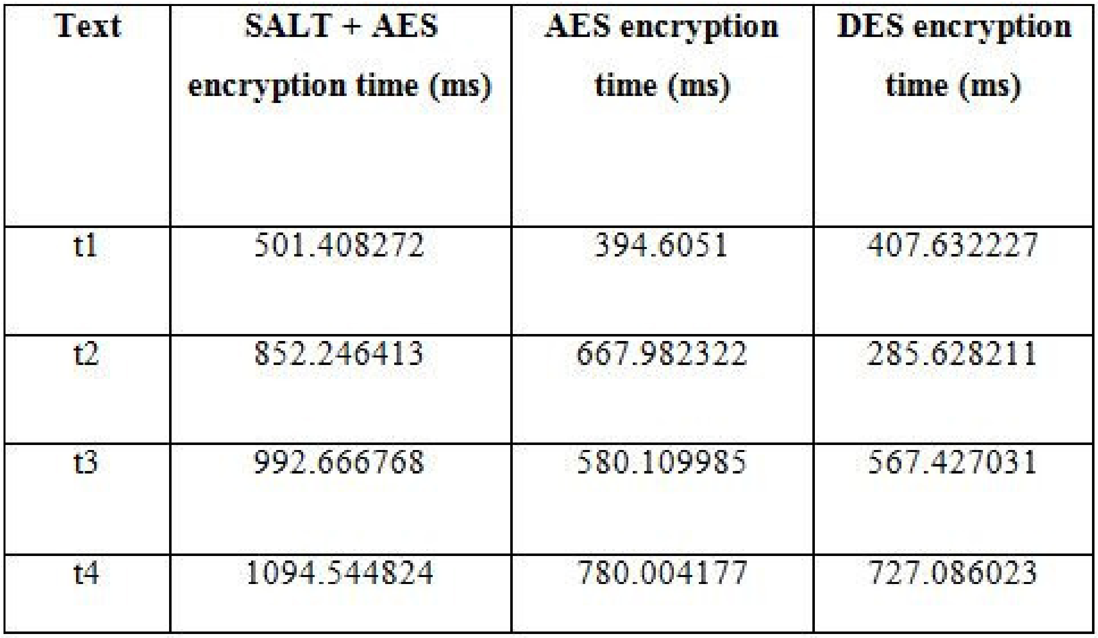


Figure 7.2 Comparison of Text size (in bytes)

2. **Encryption Time,** time taken to convert plai text to cipher text [40]. Table 7.3 and Figure 7.3 show the comparison between the encryption time among SALT + AES cipher, AES cipher and DES cipher.

Table 7.3 Comparison of Encryption Time (in ms)



Text	SALT + AES encryption time (ms)	AES encryption time (ms)	DES encryption time (ms)
t1	501.408272	394.6051	407.632227
t2	852.246413	667.982322	285.628211
t3	992.666768	580.109985	567.427031
t4	1094.544824	780.004177	727.086023

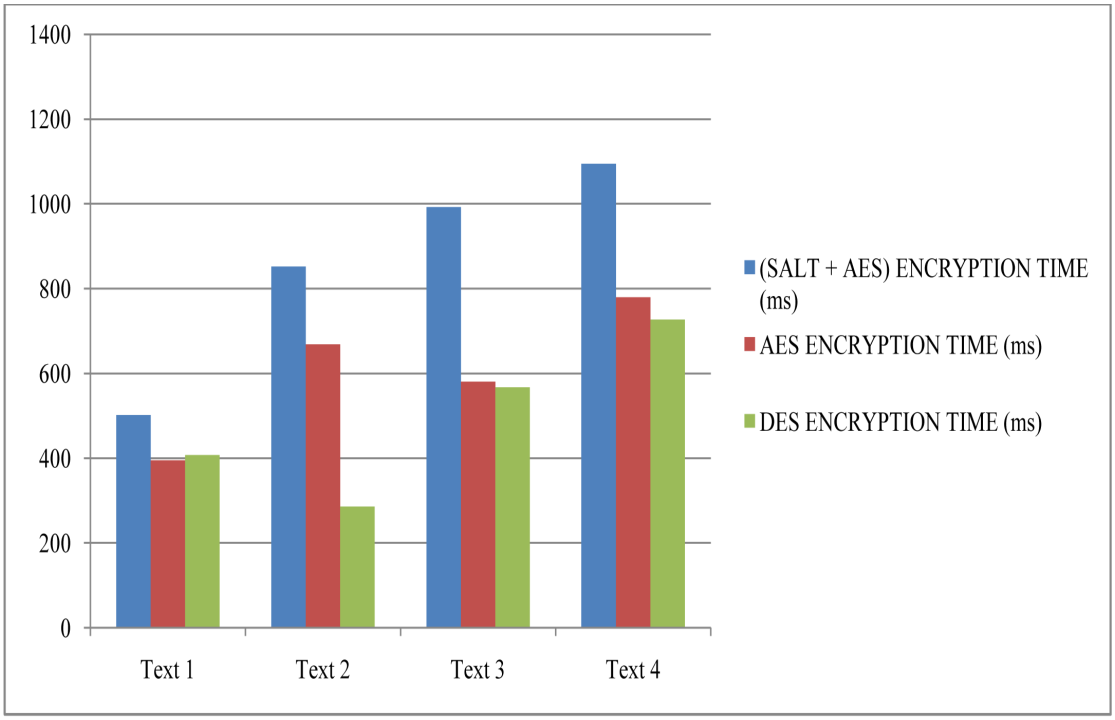
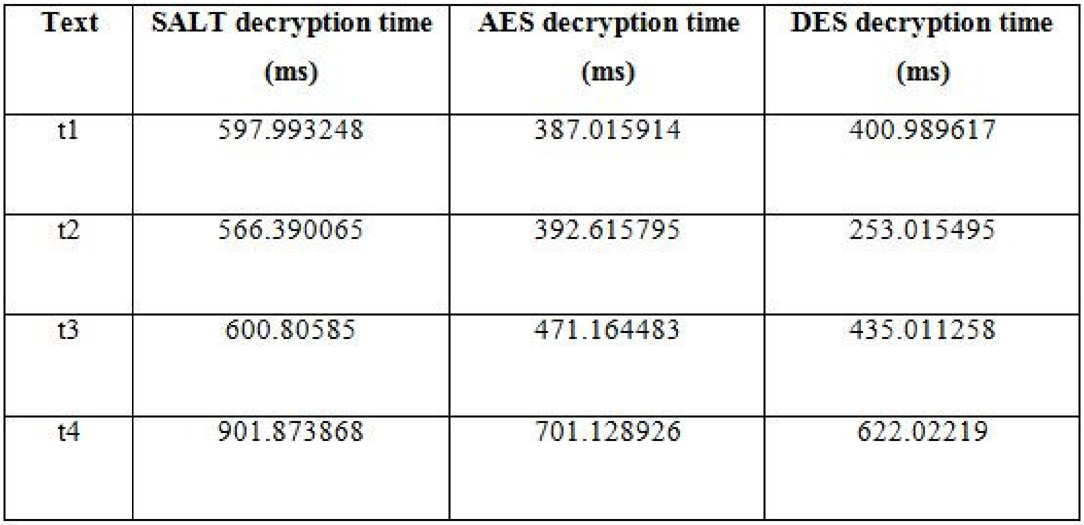


Figure 7.3 Comparison of Encryption Time (in ms)

3. **Decryption Time,** time taken to convert cipher text back to plain text [40]. Table 7.4 and Figure 7.4 show the comparison between the decryption time among SALT + AES cipher, AES cipher and DES cipher.

Table 7.4 Comparison of Decryption Time (in ms)



Text	SALT decryption time (ms)	AES decryption time (ms)	DES decryption time (ms)
t1	597.993248	387.015914	400.989617
t2	566.390065	392.615795	253.015495
t3	600.80585	471.164483	435.011258
t4	901.873868	701.128926	622.02219

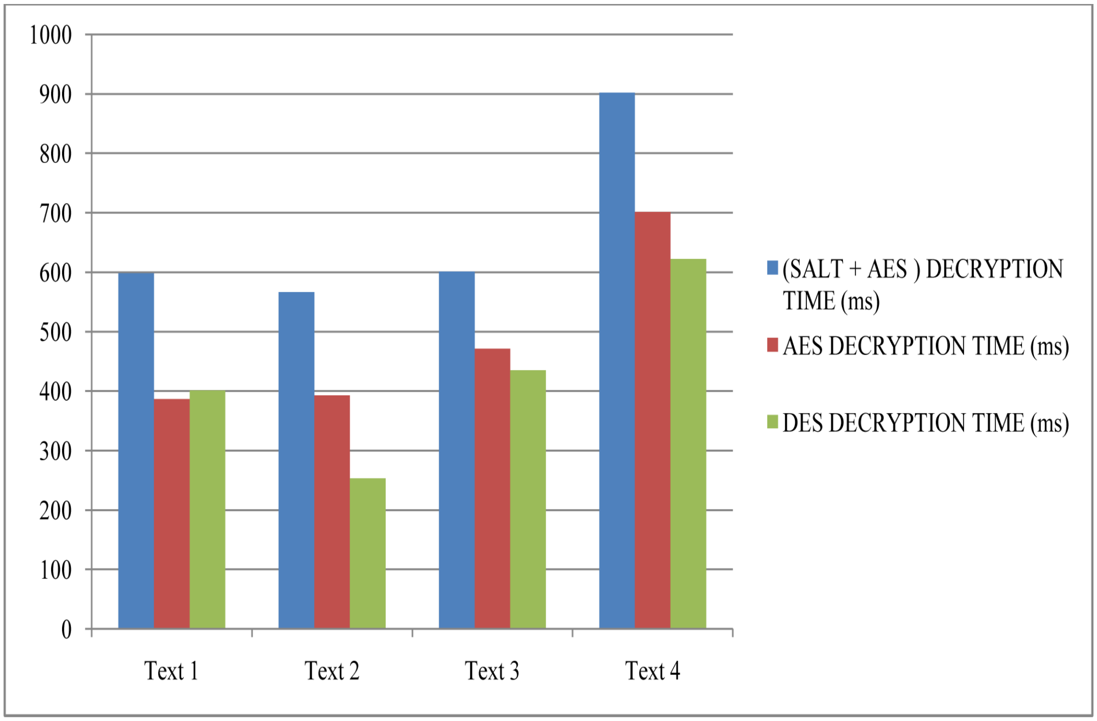


Figure 7.4 Comparison of Decryption Time (in ms)

CHAPTER 8
CONCLUSION/FUTURE SCOPE

8.1 CONCLUSION

Mobile Crowdsourcing has evolved as very powerful and effective method of gathering information from the crowd. Even after many advantages it still faces some drawbacks. The objective of this study was to identify the issues of crowdsourcing that were security, privacy and trust. Further out these three issues two were focused upon that was trust and privacy issue.

For trust issue DST was proposed as a solution for trust issue. The algorithm showed the probability of something being certain, uncertain or maybe certain and thus helped to identify the trust level.

For privacy issue combination of SALT cryptography and AES was used. Random alphabets were added as SALT to the password or any personal data after that hash function was applied further AES was applied. For result purpose this cryptography was compared with normal AES and DES and the result showed that the cipher text was of bigger bytes then the cipher text of AES and DES thus making it difficult for the attackers to crack.

8.2 FUTURE SCOPE

As far as future scope is concerned DST & SALT cryptography can be used or applied to many other datasets and even to real time application for the verification of data.

REFERENCES

[1] K. Mao, L. Capra, M. Harman, and Y. Jia, Y, “A survey of the use of crowdsourcing in software engineering,” Journal of Systems and Software, vol. 126, pp. 57-84, 2017.

[2] Y. Wang, X. Jia, Q. Jin and J. Ma, “Mobile crowd sourcing: Architecture, applications, and challenges,” In Proceedings of UIC-ATC-ScalCom-CBDCom-IoP, IEEE, pp. 1127-1132, 2015.

[3] J. Phuttharak, and S.W. Loke, “Mobile crowd sourcing in peer-to-peer opportunistic networks: energy usage and response analysis,” Journal of Network and Computer Applications, vol. 66, pp. 137-150, 2016.

[4] W. Feng, Z. Yan, H. Zhang, K. Zeng, Y. Xiao, and Y.T. Hou, “A Survey on Security, Privacy and Trust in Mobile Crowdsourcing,” IEEE Internet of Things Journal, 2017.

[5] N. Sharma, R. Rathi, V. Jain and M.W. Saifi, “A novel technique for secure information transmission in videos using salt cryptography,” In Engineering (NUiCONE), 2012 Nirma University International Conference on IEEE, pp. 1-6, 2012.

[6] H. Lin, M. Schwartz, J. Michalski, M. Shakamuri, and P. Campbell, “Leveraging a crowd sourcing methodology to enhance supply chain integrity,” In Security Technology (ICCST), 2012 IEEE International Carnahan Conference on IEEE, pp 27-33, 2012.

[7] A.C. Weaver, J.P. Boyle, and L.I. Besaleva, “Applications and trust issues when crowdsourcing a crisis,” In Computer Communications and Networks (ICCCN), 2012 21st International Conference on IEEE, pp. 1-5, 2012.

[8] Y. Liu, and M. Liu, “An online learning approach to improving the quality of crowd-sourcing,” In ACM SIGMETRICS Performance Evaluation Review, vol. 43, pp. 217-230, 2015.

[9] J. Ren, Y. Zhang, K. Zhang, and X.S. Shen, “SACRM: Social aware crowdsourcing with reputation management in mobile sensing,” Computer Communications, vol. 65, pp. 55-65, 2015.

[10] S. Joshi, and D.K. Mishra, “A roadmap towards trust management & privacy preservation in mobile ad hoc networks,” In ICT in Business Industry & Government (ICTBIG), International Conference on IEEE, pp. 1-6, 2016.

[11] S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H. Katz, “An architecture for a secure service discovery service,” In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking ACM, pp. 24-35, 1999.

[12] N.B. Priyantha, A.K. Miu, H. Balakrishnan, and S. Teller, “The cricket compass for context-aware mobile applications,” In Proceedings of the 7th annual international conference on Mobile computing and networking ACM, pp. 1-14, 2001.

[13] N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” In Proceedings of the 2nd ACM workshop on Wireless security ACM, pp. 1-10, 2003.

[14]Y. Zhang, Z. Li, and W. Trappe, “Power-modulated challenge-response schemes for verifying location claims,” In Global Telecommunications Conference, GLOBECOM'07.IEEE, pp. 39-43, 2007.

[15] S. Saroiu, and A. Wolman, “Enabling new mobile applications with location proofs,” In Proceedings of the 10th workshop on Mobile Computing Systems and Applications ACM, pp. 1-3, 2009.

[16] P. Gilbert, L.P. Cox, J. Jung, J. and D. Wetherall, “Toward trustworthy mobile sensing,” In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications ACM, pp. 31-36, 2010.

[17] S. Saroiu, and A. Wolman, A., “I am a sensor, and I approve this message,” In Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications ACM, pp. 37-42, 2010.

[18] H. Amintoosi, and S.S. Kanhere, “A trust framework for social participatory sensing systems,” In International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services Springer, Berlin, Heidelberg, pp. 237-249, 2012.

[19] T. Luo, S.S. Kanhere, and H.P. Tan, “SEW-ing a simple endorsement web to incentivize trustworthy participatory sensing,” In Sensing, Communication, and Networking (SECON), Eleventh Annual IEEE International Conference on IEEE, pp. 636-644, 2014.

[20] C. Wu, T. Luo, F. Wu, and G. Chen, “EndorTrust: An endorsement-based reputation system for trustworthy and heterogeneous crowdsourcing,” In Global Communications Conference (GLOBECOM), IEEE, pp. 1-6, 2015.

[21] Y. Gong, Y. Guo and Y. Fang, "A privacy-preserving task recommendation framework for mobile crowd sourcing," In Global Communications Conference (GLOBECOM), IEEE, pp. 588-593, 2014.

[22] Y. Gong, L. Wei, Y. Guo, C. Zhang and Y. Fang, "Optimal task recommendation for mobile crowd sourcing with privacy control," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 745-756, 2016.

[23] R. Liu, J. Cao, L. Yang and K. Zhang, "Priwe: Recommendation for privacy settings of mobile apps based on crowd sourced users' expectations," In Mobile Services (MS), 2015 IEEE International Conference on IEEE, pp. 150-157, 2015.

[24] C.M. Tseng and C.K. Chau, "On the privacy of crowd-sourced data collection for distance-to-empty prediction and eco-routing," In Proceedings of the Workshop on Electric Vehicle Systems, Data, and Applications ACM, pp. 1-3, 2016.

[25] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," Computer Networks, vol. 102, pp. 157-171, 2016.

[26] B. Zhang, C.H. Liu, J. Lu, Z. Song, Z. Ren, J. Ma and W. Wang, "Privacy-preserving QoI-aware participant coordination for mobile crowdsourcing," Computer Networks, vol. 101, pp. 29-41, 2016.

[27] T. Kandappu, A. Misra, S.F. Cheng and H.C. Lau, "Privacy in context-aware mobile crowd sourcing systems," In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on IEEE, pp. 231-236, 2017.

[28] J.H. Ziegeldorf, M. Henze, J. Bavendiek and K. Wehrle, "TraceMixer: Privacy-preserving crowd-sensing sans trusted third party," In Wireless On-demand Network Systems and Services (WONS), 2017 13th Annual Conference on IEEE, pp.17-24, 2017.

[29] L.L. Zhang, C.J.M Liang, Z.L. Li, Y. Liu, F. Zhao and E. Chen, "Characterizing privacy risks of mobile apps with sensitivity analysis," IEEE Transactions on Mobile Computing, vol. 17, no. 2, pp. 279-292, 2018.

[30] A.C. Myers and B. Liskov, "Protecting privacy using the decentralized label model," ACM Transactions on Software Engineering and Methodology (TOSEM), vol. 9, no. 4, pp. 410-442, 2000.

[31] W. Enck, P. Gilbert, S. Han, V. Tendulkar , B.G. Chun, L.P. Cox, J. Jung, P. McDaniel and A.N. Sheth, “TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones,” ACM Transactions on Computer Systems (TOCS), vol. 32, no. 2, pp. 5, 2016.

[32] A.R. Beresford, A. Rice, N. Skehin and R. Sohan, “Mockdroid: trading privacy for application functionality on smartphones,” In Proceedings of the 12th workshop on mobile computing systems and applications ACM, 2011.

[33] J. Lin, S. Amini, J.I. Hong, N. Sadeh, J. Lindqvist and J. Zhang, “Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing,” In Proceedings of the 2012 ACM Conference on Ubiquitous Computing ACM, pp. 501-510, 2012.

[34] Y. Agarwal and M. Hall, “ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing,” In Proceeding of the 11th annual international conference on Mobile systems, applications, and services ACM, pp. 97-110, 2013.

[35] Chen X, Wu X, Li XY, He Y and Liu Y (2014) Privacy-preserving high-quality map generation with participatory sensing. In INFOCOM, 2014 Proceedings IEEE. 2310-2318.

[36] Yao Y, Yang LT and Xiong NN (2015) Anonymity-based privacy-preserving data reporting for participatory sensing. IEEE Internet of Things Journal. 2(5):381-390.

[37] S. Gisdakis, T. Giannetsos and P. Papadimitratos, “Security, privacy, and incentive provision for mobile crowd sensing systems,” IEEE Internet of Things Journal, vol. 3, no. 5, pp. 839-853, 2016.

[38] J. Liao, Y. Bi, and C. Nugent, “Activity recognition for Smart Homes using Dempster-Shafer theory of Evidence based on a revised lattice structure,” In Intelligent Environments (IE), 2010 Sixth International Conference on IEEE, pp. 46-51, 2010.

[39] S. Liu, A.C. Kot, C. Miao, and Y.L. Theng, “A dempster-shafer theory based witness trustworthiness model to cope with unfair ratings in e-marketplace,” In Proceedings of the 14th annual international conference on electronic commerce ACM, pp. 99-106, 2012.

[40] P.P. Churi, V. Ghate, and K. Ghag, “Jumbling-Salting: An improvised approach for password encryption,” In Science and Technology (TICST), 2015 International Conference on IEEE, pp. 236-242, 2015.