Implementation of Jagruti App-Evidence by

Anoymous

Chaitali Shidunkar, Saili Mhatre, Akshay Mohite

[*chaitalishidunkar@gmail.com*](mailto:chaitalishidunkar@gmail.com) *,* [*sailinirmala1970@gmail.com*](mailto:sailinirmala1970@gmail.com) *,* [*39akshaymohite@gmail.com*](mailto:39akshaymohite@gmail.com)

Datta Meghe College of Engineering ,Airoli ,Navi-Mumbai.

Mumbai University.

*Abstract*— **Everyday crimes occur should be known to each and**

**every person. Garbage, water problems, sanitation, power supply etc., municipal issues are a common site every day and crimes exist in various forms everywhere. But people don't readily come forward for reporting these issues due to the fear of revealing oneself. Therefore, we are proposing such a system that will help people to present their issues without any fear. Registering complaint about a civic issue is now just an App away. The prime objective of. The proposed system is to preserve the privacy of people while they are reporting for any of the problems which we discussed earlier. With smart phones becoming increasingly popular, citizens can now download any Android applications at any-time since they are cost efficient and easily available. Hence, we are developing an Android Application which is very helpful for the people to come against any issues they might be facing.**

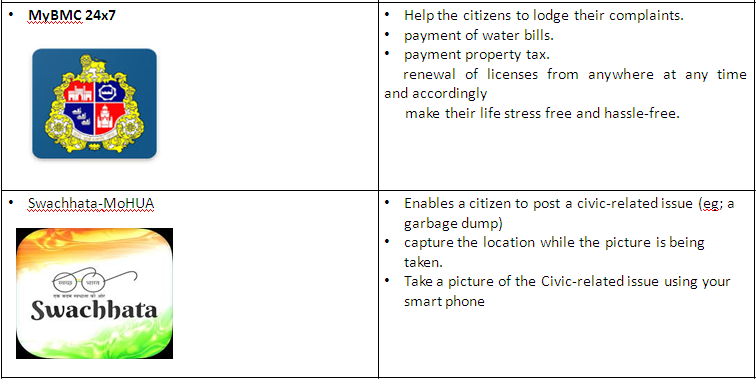
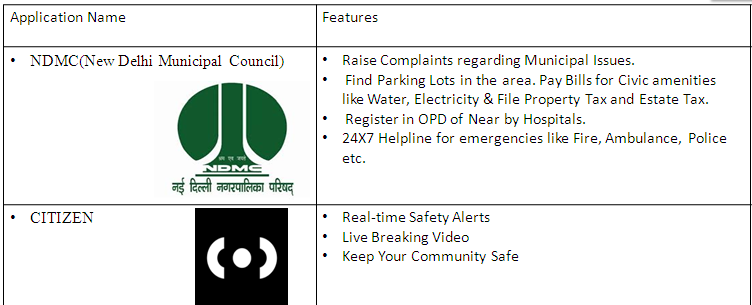
**Index Terms — Location sensing, Shamir’s Algorithm.**

I. INTRODUCTION

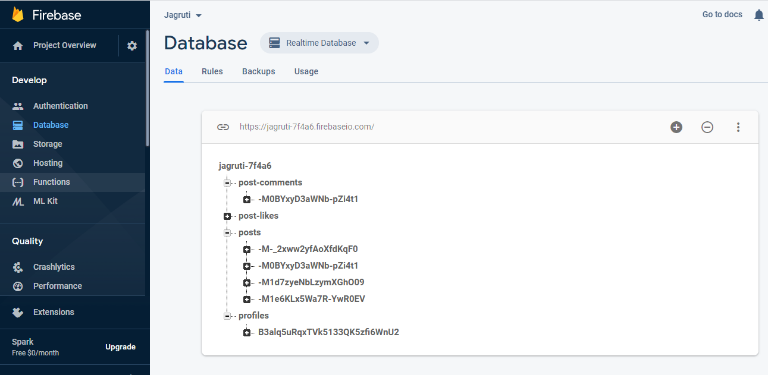
We are living in the 21st century so called as the modern century, as a member of this century we all have seen many technological developments in the field of Information and Technology. Development in the technology has led to a more comfortable lifestyle but still there are many general problems which are not yet been solved. Problems involving municipal related issues and crimes are increasing at a higher rate. Everyday crimes occur should be known to each and every person. Garbage, water problems, sanitation, power supply etc., municipal issues are a common site every day and crimes exist in various forms everywhere. But people don't readily come forward for reporting these issues due to the fear of revealing oneself. Therefore, we are proposing such a system that will help people to present their issues without any fear. Registering a complaint about a civic issue is now just an App away. The prime objective of the proposed system is to preserve the privacy of people while they are reporting for any of the problems which we discussed earlier. With smart phones becoming increasingly popular, citizens can now download any Android applications at any-time since they are cost efficient and easily available. Hence, we are developing an Android Application which is very helpful for the people to come forward and raise their voice against any issues (which are discussed above) they might be facing. Using our proposed Android Application people can lodge complaints and report incidents such as criminal incidents. The techniques used in our system are Shamir's Secret Sharing Algorithm for encryption purpose to preserve identity of users. Citizens can not only make a complaint on several issues using the application but they can also upload photographs of the civic problem. After registering on the application, the user can make complaints regarding garbage, cattle, potholes and street lights. User can also report incidents that are dedicated to social issues like lost items, events, local crime spotting,etc.

The rest of the paper is organized as follows. Section II describes our data and collection method. In Section III, we show the temporal patterns of different venue categories. In Section IV, usage of Shamir’s algorithm. In Section V, usage of APIs for login, storage and authentication purpose. In Section VI, usage of app b normal user. Finally, we conclude our work and discuss some future work.

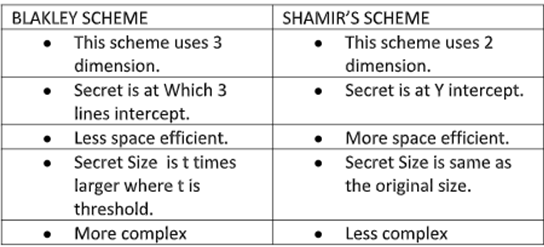
* 1. BACKGROUND AND DATA COLLECTION



B. Data Collection

Our data collection has three parts. The first is to collect the information related to simiar apps available on Play-Store but also survey for the disadvantages of those apps and then second one is to find out how to overcome them so that there is much better awareness among public .And finally survey for the algorithms which can be used to implement our application. Different login API’ s is also provided so we have to use the google-APIs like Facebook and Gmail. Also, for location purpose we will be use google-maps API in our application. For storage purpose whether Firebase or Sqlite will be better had to be surveyed. So finally, as our app is distributed one means the posts from users will be in dynamic and distributed form hence, Firebase was the solution for database purpose. 

Also, information related to Secret Sharing -algorithm we surveyed and got 2 algorithms they were Blakeley algorithm and Shamir Algorithm. But amongst them Shamir was useful and efficient in storage and complexity purpose.



III. VISUALIZATION OF TEMPORAL DATA TRAFFIC

In our application the users after registering in the application will be able to post any municipal or criminal related issues and facts .This posts can be liked, reviewed, rated, commented by many users who can see those posts. And hence , spread awareness among people without any fear of revealing their identity to public .It is useful to spread awareness amongst people without any fear of getting threatened by any higher authority. And this identity hiding is done using Shamir’s secret sharing algorithm used in our app.

a0=1234, a1=166, a2=94, where a0 is secret.

Our polynomial to produce secret shares (points) is therefore:

f(x)=1234+166x+94x2

{\displaystyle f(x)=1234+166x+94x^{2}\,\!}We construct six points {\displaystyle D\_{x-1}=(x,f(x))} from the polynomial:

D0=(1,1494),D1=(2,1942),D2=(3,2578),D3=(4,3402),D4=(5,4414),D5=(6,5614)

{\displaystyle D\_{0}=(1,1494);D\_{1}=(2,1942);D\_{2}=(3,2578);D\_{3}=(4,3402);D\_{4}=(5,4414);D\_{5}=(6,5614)\,\!}We give each participant a different single point This is necessary because {\displaystyle f(0)} f (0) is the secret.

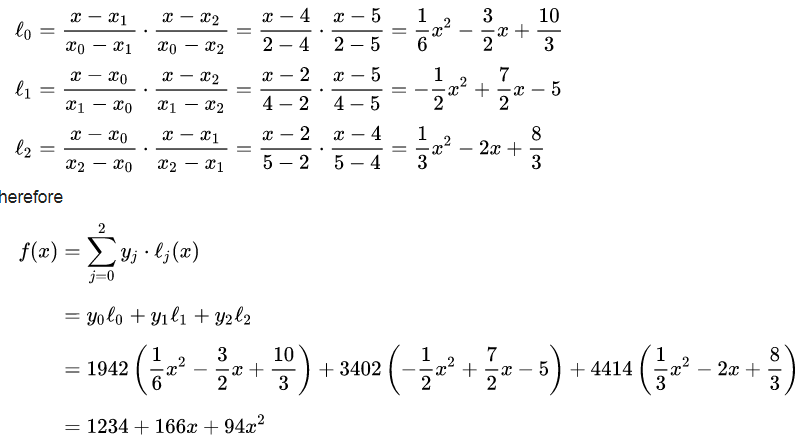
#### Reconstruction

In order to reconstruct the secret any 3 points will be enough .Consider,

(x0, y0) =(2,1942), (x1,y1)=(4,3402),(x2,y2)=(5,4414)

{\displaystyle \left(x\_{0},y\_{0}\right)=\left(2,1942\right);\left(x\_{1},y\_{1}\right)=\left(4,3402\right);\left(x\_{2},y\_{2}\right)=\left(5,4414\right)\,\!}.We will compute [Lagrange basis polynomials](https://en.wikipedia.org/wiki/Lagrange_polynomial):{\displaystyle \ell \_{0}={\frac {x-x\_{1}}{x\_{0}-x\_{1}}}\cdot {\frac {x-x\_{2}}{x\_{0}-x\_{2}}}={\frac {x-4}{2-4}}\cdot {\frac {x-5}{2-5}}={\frac {1}{6}}x^{2}-{\frac {3}{2}}x+{\frac {10}{3}}\,\!}{\displaystyle \ell \_{1}={\frac {x-x\_{0}}{x\_{1}-x\_{0}}}\cdot {\frac {x-x\_{2}}{x\_{1}-x\_{2}}}={\frac {x-2}{4-2}}\cdot {\frac {x-5}{4-5}}=-{\frac {1}{2}}x^{2}+{\frac {7}{2}}x-5\,\!}

{\displaystyle \ell \_{2}={\frac {x-x\_{0}}{x\_{2}-x\_{0}}}\cdot {\frac {x-x\_{1}}{x\_{2}-x\_{1}}}={\frac {x-2}{5-2}}\cdot {\frac {x-4}{5-4}}={\frac {1}{3}}x^{2}-2x+{\frac {8}{3}}\,\!}Therefore, {\displaystyle {\begin{aligned}f(x)&=\sum \_{j=0}^{2}y\_{j}\cdot \ell \_{j}(x)\\[6pt]&=y\_{0}\ell \_{0}+y\_{1}\ell \_{1}+y\_{2}\ell \_{2}\\[6pt]&=1942\left({\frac {1}{6}}x^{2}-{\frac {3}{2}}x+{\frac {10}{3}}\right)+3402\left(-{\frac {1}{2}}x^{2}+{\frac {7}{2}}x-5\right)+4414\left({\frac {1}{3}}x^{2}-2x+{\frac {8}{3}}\right)\\[6pt]&=1234+166x+94x^{2}\end{aligned}}}Recall that the secret is the free coefficient, which means that {\displaystyle S=1234\,\!}, and we are done.



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| IV. SHAMIR SECRET SHARING ALGORITHM Preparation Suppose that our secret is 1234 {\displaystyle (S=1234)\,\!}.We wish to divide the secret into 6 parts (n=6) {\displaystyle (n=6)\,\!}, where any subset of 3 parts (k=3) {\displaystyle (k=3)\,\!} is sufficient to reconstruct the secret. At random we obtain k-1 {\displaystyle k-1} numbers: 166 and 94.  a0=1234, a1=166, a2=94, where a0 is secret.  Our polynomial to produce secret shares (points) is therefore:  f(x)=1234+166x+94x2  Suppose that our secret is 1234 {\displaystyle (S=1234)\,\!}.We wish to divide the secret into 6 parts (n=6) {\displaystyle (n=6)\,\!}, where any subset of 3 parts (k=3) {\displaystyle (k=3)\,\!} is sufficient to reconstruct the secret. At random we obtain k-1 {\displaystyle k-1} numbers: 166 and 94. | | | | | | |  | | | | | | | |  |
|  |  |  |  |  |  |  |  | | | | | | | |  |

VI. RELATED WORK

In our application we used algorithm that is Shamir Seceret Sharing Algorithm for identity hiding as explained in above section. For authentication purpose we provided two ways to login for user i.e.,via Gmail and via Facebook. For this we required Google APIs for both the logins. Also for storage purpose we used firebase as sqlite is useful only for limited no of users and also for offline purpose. Firebase is for distributed and dynamic system. All the information related to user personal information or posts that he/she posted is stored on cloud using Firebase.

VII. CONCLUSION AND DISCUSSIONS

The problem of criminal activities and municipal issues is increasing rapidly day by day, so we can develop such an application for altering the concerned issues which can help us to stop such type of illegal activities. We can also make people aware of any facts happening anywhere and also make people fearless about spreading social awareness as their identity is not revealed.

ACKNOWLEDGEMENT

This research was supported/partially supported by our team members and a research paper called Shamir’s Secret Sharing Algorithm. We would also like to show our gratitude to the (Madhura Phadke, project Guide, Datta Meghe College of Engineering) for sharing their pearls of wisdom with us during the course of this research, and we thank 3 “anonymous” reviewers for their so-called insights. We are also immensely grateful to (List names and positions) for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed persons...

REFERENCES

1. F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida. Characterizing User Behavior in Online Social Networks. In Proc. of ACM SIGCOMM, 2009.
2. T. Hu, E. Bigelow, J. Luo, and H. Kautz. Tales of Two Cities: Using Social Media to Understand Idiosyncratic Lifestyles in Distinctive Metropolitan Areas. IEEE Transactions on Big Data, 3(1):55–66, 2017.
3. L. Jin, Y. Chen, T. Wang, P. Hui, and A. V. Vasilakos. Understanding User Behavior in Online Social Networks: A Survey. Communications Magazine, IEEE, 51(9):144–150, 2013.
4. A. Noulas, S. Scellato, N. Lathia, and C. Mascolo. Mining User Mobility Features for Next Place Prediction in Location-based Services. In Proc. of ICDM. IEEE, 2012.
5. Alorithm<https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing>
6. <http://www.ijsrp.org/research-paper-0413/ijsrp-p16122.pdf> for understanding the algorithm porperly.