Public bulletin boards for integrity of electoral rolls

Prashant Agrawal Subodh Sharma Subhashis Banerjee

Email: {prashant,svs,suban}@cse.iitd.ac.in

Computer Science and Engineering
IIT Delhi
New Delhi 110016, India

April 5, 2021

Abstract

Democracy principles demand that the integrity of electoral rolls should be publicly verifiable. In this note we suggest the use of append-only, immutable public bulletin boards for transparent and tamper-proof maintenance of electoral roll data whose authenticity can be verified by all interested and eligible parties.

In a recent report of the Citizens' Commission on Elections, Mander and Ramani [Mander and Ramani, 2021] have pointed out several problems of exclusion and disenfranchisement that plague the electoral rolls in India. Whereas processes for inclusion - proactively identifying all eligible voters and making sure that they are able to vote, irrespective of whether they apply or not - require being particularly mindful of marginalised communities and careful process design at local community levels, some of the other problems related to exclusion and duplicate entries can be addressed by transparent and effective data processing. In this note we make some suggestions for organisation and processing of electoral roll data that may ensure that

1. all applications for inclusion in electoral rolls - whether by voters themselves, or by their representatives on their behalf - are correctly processed
2. there are no spurious deletions from the electoral rolls
3. there are no duplicate or false entries in the electoral rolls.

We propose to ensure the integrity of the electoral rolls by maintaining records in a manner that enables complete transparency and public verifiability of all decisions regarding enrolment, updates and deletions. We also briefly comment on the suitability of *blockchain* technology [Mearian, 2019] for electoral rolls and other electoral data, which apparently is being seriously contemplated by the ECI [Mishra, 2020].

Maintaining electoral records on public bulletin boards

For transparency and verifiability of records, we recommend using the construct of an append-only, immutable (tamper-proof) public (web) bulletin board [Heather and Lundin, 2009], in which data can only be added but never deleted. A public bulletin board - a publicly readable sequence of bulletins $\langle B_1, B_2, \ldots, B_n \rangle$ - can be defined in terms of the following properties:

Certified publishing: A public (web) bulletin board has certified publishing if whenever readers retrieve the contents of the board, for each bulletin on the board they can determine with certainty (obtain a formal proof of):

1. the identity of the (sub) authority that published the bulletin.
2. the time of the publication within a pre-specified bound.

Failure to determine either of the above with certainty will indicate malfeasance or corruption of the bulletin board.

Unalterable history: A web bulletin board has unalterable history if, whenever a reader retrieves the contents of the board at any time T_0 and again at any later time T_1, she is able to verify that the board read at T_1 has exactly the same content as previously at T_0 (it is untampered), except for possibly having some additional new messages appended at the end (that is, the board at T_0 is a prefix of the board at T_1). If this is not the case, it indicates malfeasance or that the board has become corrupted.

We suggest that the Election Commission of India (ECI) should maintain two public bulletin boards for each constituency - at a block/ward level granularity - which should be updated as and when changes occur.

1. **Bulletin board of electoral rolls:** This should be a self-contained bulletin board of the entire electoral roll - updated with all additions, deletions and changes till date - where each entry is dated and digitally signed by a competent authority in the ECI. This should be the official master electoral roll correct up to the time of the last update, and the list of valid voters on any date can be publicly determined from this bulletin board.

2. **Bulletin board of transaction records:** This should contain

   (a) the sequence of all enrolment applications received and enrolment records generated by the Electoral Registration Officers (ERO), and the processing information including reasons for acceptance or rejection

   (b) the sequence of all change or deletion requests generated, and the processing information clearly citing the reasons for the change or deletion

   For every application of enrolment, update or deletion, the concerned authority in the ECI should issue a digitally signed receipt - a commitment - using which a voter (or her representative) should be able to search for her application processing status on the bulletin boards. Missing processing information for a committed receipt will indicate a failure of the ECI to fulfil an obligation. Every entry in the append-only bulletin boards should be time stamped and digitally signed by a concerned competent authority. Any member of the public should be able to verify the authenticity and the integrity of the bulletin boards. Authorised entities (may even be everybody) should be able to carry out search, deduplication and audit operations on the bulletin boards.

Privacy of electoral records

There is always an inherent tension between privacy and public transparency. The public web bulletin boards may be made privacy preserving by replacing the clear text messages on the bulletin boards with their cryptographic hashes (see the section below) computed using a suitable publicly committed hash function. Publishing the hashes will ensure that the original messages cannot be altered, and access to the unalterable original messages may only be given to a restricted set of authorised entities - including representatives of political parties - after authentication.

It is to be noted that there is no theory to substantiate that publishing only image records of electoral rolls - as is the current practice of the ECI - protects privacy, and it only serves to make searching the database difficult for an honest operator.

Some basic technical background for secure and searchable append-only public bulletin boards

In what follows we briefly describe the broad technical specifications of such immutable and transparent bulletin boards. We include it here for completeness, and a not-so-interested-in-these-details reader may skip this section.

The construction of a public bulletin board is based on two technical concepts from computer science:

1. **Digital signature:** The digital signature $s = \textbf{sign}(msg, sk)$ of a message msg is signed using a publicly known function **sign** and a secret key sk, and it can be verified using a publicly known function **verify**(msg, s, pk) which returns either *true* or *false*, using the public key pk of the signing authority. A digital signature is non-repudiable and the signature and the integrity of the message can be publicly verified by anybody using the pre-published public key of the signer.

2. **Hash function:** A hash $h = H(msg)$ of a message msg is computed using a hash function H. The hash function is *one-way* if given a hash value h it is computationally difficult (almost impossible) to find a msg such that $h = H(msg)$; and is *collision resistant* if finding msg_1 and msg_2 such that $H(msg_1) = H(msg_2)$ is computationally difficult. The above two properties guarantee that once the hash of a message is published, it becomes practically impossible to alter the message.

Using the above, a public bulletin board may be realised by requiring that for each bulletin B_i

$$B_i = (m_i, T_i, W_i, h_i, WSign_i, BSign_i)$$

where m_i is the message of the bulletin and must contain a searchable reference to an issued receipt or a commitment, T_i is the writer's timestamp, W_i is the identity of the writer (the sub-authority of ECI that is posting the message), h_i is a hash computed by any suitable publicly committed cryptographically secure one-way and collision resistant hash function H, $WSign_i$ and $BSign_i$ are signed terms as described below. The bulletins must satisfy the following *invariant*:

1. $h_i = H(m_i \cdot T_i \cdot W_i \cdot h_{i-1})$; where $h_0 = 0$ and $\cdot$ is the string concatenation operator.
2. $WSign_i = SW_i(h_i)$; where $SW_i()$ indicates signing with the private key of the writer.
3. $BSign_i = SB_i(WSign_i \cdot T'_i)$; where $SB_i()$ indicates signing with the private key of the bulletin board, and T'_i is the bulletin board's timestamp at the time of signing, which must be within a bounded small delay after the writer's timestamp.

The above will have protection against insertion, deletion and alteration of messages even if the writers and the bulletin board collude [Heather and Lundin, 2009]. If the writer and the bulletin board maintainer are the same authority (not recommended; the bulletin board may be maintained by an independent agency, or even multiple independent agencies) then it will be necessary for some readers to read whenever there is an update (or at least once in a while), or for the bulletin board to push out (upload) the differential bulletin board content to some neutral place. Concurrency control for multiple writers may be realised by serializing using standard distributed computing protocols.

The requirements outlined above constitute a special case where all writing authorities are sub-jurisdictions of the ECI and there is no possibility of any conflict in the time order of writing records, and the requirements of precise timing of reading and writing are somewhat relaxed.

Public bulletin boards versus *blockchain*

When ECI is the sole authority to decide on the information to be displayed on the bulletin boards, there is no need for any distributed consensus among multiple parties for committing content on the bulletin board, as, for example, in a *blockchain* [Mearian, 2019]. In fact, a *blockchain* based solution where there is only one authority is actually highly insecure because a *blockchain* derives its security from distributed control through multiple mutually adversarial entities.

In contrast, in this situation, the ECI is obligated to post processing status reports for all service requests. The ECI needs to make a commitment for all such requests by issuing a digitally signed receipt or a certificate, so there is no possibility of omission of records. It just needs to post all follow up information on public bulletin boards in a tamper-proof and non-repudiable (even by and insider) manner.

Conclusion

We have presented a simple data organisation framework for maintaining the integrity of electoral rolls. The hash chain based public bulletin board protocol should be straightforward to implement. Similar public bulletin boards may also be considered for maintaining applications and processing records of out-of-station voters if and when a remote voting scheme for migrant voters is implemented.

References

James Heather and David Lundin. The append-only web bulletin board. In Pierpaolo Degano, Joshua Guttman, and Fabio Martinelli, editors, *Formal Aspects in Security and Trust*, pages 242–256, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. ISBN 978-3-642-01465-9. URL https://epubs.surrey.ac.uk/107392/5/append-only.pdf.

Harsh Mander and Venkatesan Ramani. Electoral Roll and Exclusi1on of Vulnerable Sections from Voting. In Justice (Retd.) Madan Lokur, Wajahat Habibullah, Justice (Retd.) Hariparanthaman, Arun Kumar, Subhashis Banerjee, Pamela Philipose, Sundar Burra, and M. G. Devasahayam, editors, *An Inquiry into India's Election System: Report of the Citizens' Commission on Elections (Volume II: Are Elections in India Free and Fair?)*. 2021. URL https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_e25fcdb755984e5b838d51f0a2badb83.pdf.

Lucas Mearian. What is blockchain? The complete guide. https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html, 2019. [Online January 30, 2019].

Shaily Mishra. Experts debate using blockchain for remote voting in India. https://www.sundayguardianlive.com/news/experts-debate-using-blockchain-remote-voting-india, 2020. [Online October 3, 2020].