A Verifiable Voting Architecture for Corporate India

Episode 72 | Big Ideas

Rajeeva Karandikar

Transcript

May 18, 2026

Rajeeva Karandikar. "A Verifiable Voting Architecture for Corporate India." Episode 72 of Big Ideas. May 18, 2026. Podcast, video, 0:26:40.
https://www.xkdr.org/viewpoints/a-verifiable-voting-architecture-for-corporate-india-big-ideas-ep-72

Abstract

India's transition to electronic voting machines (EVMs) in 2004 marked a significant shift from paper-based elections, but digital voting has quietly expanded far beyond parliamentary elections into corporate boardrooms and professional societies. Professor Rajeeva Karandikar reveals how COVID-19 accelerated the adoption of electronic voting for annual general meetings and corporate governance, creating new challenges around verification and trust that current systems cannot adequately address.

The conversation explores a fundamental problem with current digital voting systems: while they eliminate the logistical nightmares of paper ballots, they create new vulnerabilities where trust must be placed entirely in the hands of the software companies conducting the polls. Karandikar proposes an innovative cryptographic solution inspired by the VVPAT (Voter Verifiable Paper Audit Trail) system used with EVMs, called User Verifiable Digital Audit Trail (UVDAT), which could enable courts to verify election results without compromising voter privacy.

This technical discussion reveals how India could lead a global transformation in digital democracy by applying lessons from international cryptography competitions to create open-source, verifiable voting systems that maintain both security and transparency.

Contents

Introduction to digital voting in India

[00:00:08] Atibhi Sharma: Hello and welcome to a brand new episode of Big Ideas.

[00:00:12] Atibhi Sharma: Today we have Professor Rajeeva Karandikar with us talking about digital voting in India.

[00:00:17] Atibhi Sharma: Professor Karandikar is an emeritus professor at Chennai Mathematical Institute and he also serves as a chairperson at National Statistics Commission.

[00:00:25] Atibhi Sharma: Welcome, professor.

[00:00:26] Rajeeva: Thank you.

[00:00:33] Atibhi Sharma: So we've seen that digital voting has taken a rise in India. It's been on the rise since 2006 when EVMs were introduced.

[00:00:39] Atibhi Sharma: What trends have you observed over the years that you can tell us about?

[00:00:43] Rajeeva: Yeah.

[00:00:44] Rajeeva: So, actually 2004 is the election when the EVMs were introduced for the entire uh, parliamentary election. Earlier there were some state elections, but really people memory is about the parliamentary election and that was 2004.

From paper ballots to EVMs in elections

[00:01:05] Rajeeva: And the need is now on the hindsight very obvious because the uh, paper voting, uh, the if one just looks at the amount of paper to be printed and distributed and so on, so forth, it was becoming increasingly high. And uh, there were all kinds of other issues involved with that voting.

[00:01:25] Rajeeva: So it was welcomed at uh early early ten years, the two two elections, it was welcomed a lot by media. Uh, off late it has been under attack and so on. But uh, but that's for another episode. Today I don't want to talk about EVM and VVPAT.

[00:01:25] Rajeeva: Uh.

[00:01:46] Rajeeva: I am my uh, talking about the electronic voting and in other context, going beyond uh, the parliamentary election or state elections, okay?

[00:01:58] Rajeeva: Um, the the in the corporate uh world, um, uh, the private corporates, public publicly listed companies, there there was a thing about annual general meeting. So any change in statutes or any policies, some broad policies had to be approved in the uh AGM. The board of directors is there, but somethings are subject to approval by AGM.

Corporate electronic voting and AGM challenges

[00:02:28] Rajeeva: And uh, with uh stakeholders or people who own the shares all across the country, uh, the number of people attending these AGMs was small and uh, so legally there was a provision for absentee ballot, paper ballot. So so there would be send a postal ballot and they will sign it and send it. Few people send, few didn't send.

[00:02:51] Atibhi Sharma: More didn't send.

[00:02:52] Rajeeva: Uh, that went on.

[00:02:55] Rajeeva: Then um, not quite electronic, but uh, the some of the companies tried getting these instead of letters via an email. Uh, because by 2010 emails had become fairly common in use by general public. And some corporates brought in uh, uh EV voting via emails. Okay?

[00:03:25] Rajeeva: And uh, that became acceptable. I think various uh, legislative bodies or the uh, which govern the uh corporates, they they agreed to this.

[00:03:41] Rajeeva: With time, with seeing the EVMs in courts and in in in parliamentary election, uh somebody had this idea of uh instead of email, because by then, it was very clear that email could be very easily to spoof. Okay?

[00:04:00] Rajeeva: Uh, or I receive an email, there is no verification. I can change. You may have voted for A, but I can edit A to B and it may appear that you have voted for B. Okay?

[00:04:00] Rajeeva: So, therefore, uh, they thought about bringing in uh different way of voting, uh electronically. And uh I won't even remember who started it, but it was kind of already there with some corporates.

[00:04:29] Rajeeva: And the uh, company law board or whichever is the appropriate authority had approved that as well. Then came COVID. Now nobody could travel for to attend the AGM, they can't even hold a AGM. So therefore it became a must.

[00:04:29] Rajeeva: And that is when uh the electronic voting, uh, so it's uh so what's the difference between this electronic voting and the voting for parliament?

[00:04:57] Rajeeva: Voting for parliament, you have to physically turn up some place and press a button. Uh this is not that. So the only name it is electronic, but otherwise it has nothing to do with the uh existing electronic voting as far as the uh parliamentary election is concerned, okay? It's voting via electronic, that's it.

[00:05:20] Rajeeva: But the mechanism put up was since emails could be easily spoofed, they had to come up with some other methodology. And uh there are at least two or three entities in India, maybe more, which did come up with some entity, some thing by which uh, the received emails could be verified, at least by that company.

[00:05:43] Rajeeva: And so the uh the the the if a at the same was applied also for societies and for other professional bodies and so on, so forth. Uh, so in that the uh as far as I know, the currently in use method is that uh some agency which conducts this poll, there could be several, they will make a bid and then uh let's say a corporate X.

[00:06:16] Rajeeva: So company X, their board approves and the law board approves that okay, such and such agency will conduct the poll for them. And uh there could be emails sent and then they have to sign the email, uh, by electronically signing, there are different methods of electronically signing a thing. From ultra legal to somewhere in between.

[00:06:40] Rajeeva: And they will go with the whole the company which is uh conducting the poll. And they will only reveal the totals to the company X which has for whom the poll is conducted. The company X will not know who voted for whom, just like in a parliamentary election. The parties will get totals, but won't get what a particular voter voted for whom because that's required.

[00:07:05] Rajeeva: But because of the methodology involved, the company which is conducting the poll, the the which has developed the source code and which is doing all this, they will have their whole data and they're it has their word for it. Okay? So via email anybody could tamper with it. Now only that entity which uh, we have to trust them, okay?

Trust and verification problems in digital voting

[00:07:29] Rajeeva: And so, during the COVID era, uh one or two entities approached me saying that uh since we know you have been involved with EVM, VVPAT, uh do you think this one is good as good as that? Is it secure?

[00:07:45] Rajeeva: And uh to that my view was that, yes, it seems to be, but we are now leaving it in the hand of the entity which has built the machine. Built the software.

[00:07:58] Rajeeva: So, going back in EVMs, the EVMs are very good. I I've interacted with the team which has designed those. But still for a third party, it was that, okay, we we trust you, but our trust we are handing it over entirely to them. That they have not uh the there is no foul play.

[00:08:18] Rajeeva: And that is why this VVPAT was introduced and VVPAT stands for Voter Verifiable Paper Audit Trail. That uh the individual voters don't get the paper, but it is stored somewhere else and if challenged, that can be counted and then the two can be matched. That is the EVM VVPAT idea. So there is a kind of a if required verifiable way.

[00:08:43] Rajeeva: And so the society which had approached me, they said that the this is what our company who is conducting it has given us. Do you think there is any way of where it can be verified in the same way? And there was no. Uh in other words, we are entirely handing over the trust to the entity which has uh, conduct written the software which conducting or the code or the app or whatever we call it, is conducting the poll for for this company X.

[00:09:17] Rajeeva: And that is when it occurred to me that uh with the privilege, it continuing to use more, what if it ends up in a court? Okay? Suppose uh a losing candidate challenges in the court that no, that company has played foul. The company which is conducted it has played foul, then what can court do?

[00:09:17] Rajeeva: There is no way that they can verify. Okay?

[00:09:43] Rajeeva: That uh that is what led to the thought that just like for while EVMs are very good, for a legal challenge, uh VVPAT was introduced. There is a need for something like that. And I even uh taking their uh leaf out of the VVPAT nomenclature, I even created a name.

[00:10:04] Rajeeva: And uh user verifiable digital audit trail. So instead of paper audit trail, the trail is also digital and instead of a voter, it's a user. Now it can be used for whatever purpose you want to use. Okay?

[00:10:04] Rajeeva: For giving an opinion, giving a voting for EV AGM, voting for uh society, voting for professional body, or if it takes off, even walking to the polling booth to cast your vote, you could but that's for future.

User verifiable digital audit trail proposal

[00:10:37] Rajeeva: But at first, if it starts getting used for uh the the corporate and for society and professional bodies, it will be a plus step and uh so so uh, it comes down to what is uh it's eventually ends up as mathematics but it's what is called cryptography.

[00:11:01] Rajeeva: Uh, just like OTP, right? Which you you you make a transaction, the you say that I want to pay so and so, so much. Uh, and the bank transfers the money and later you say, I have not said. So they have to have a say that no, you have said it.

[00:11:01] Rajeeva: Right? So it's not only have to be correct, they have to be able to the bank has to be able to prove to the court if required that it was your instruction.

[00:11:27] Rajeeva: So that is based on uh some form of cryptography and so a combination, okay? That bank has to be able to prove that they sent this OTP to your phone number and you put that in back. Okay? Things like that.

[00:11:45] Rajeeva: So, uh there is a need for a system by which the entity conducting the poll can give the totals to the client, but if challenged can prove to in the court of law that they have not played foul. They have actually given the right count. Okay? And how to do that is the question.

[00:12:08] Rajeeva: Now, there can be multiple ways, okay? And uh uh in the Indian context, right now I'm talking Indian context. It can be taken globally later because uh the folks from abroad when they come and see the digital transformation India, they are amazed. Right?

[00:12:08] Rajeeva: But uh so let's make it, I mean we have enough of need for this. Let's make it work here and then we can see if internationally people are interested.

Implementation approaches and cryptographic standards

[00:12:38] Rajeeva: So, there could be multiple ways. One could be that uh the the one of the government entities, either the Ministry of Corporate affairs, one of the entities can float as a, they can call for proposals. Yeah. Okay?

[00:12:38] Rajeeva: And uh multiple people can give proposals and then they have a team which evaluates that and tries to pick one or two or they can verify even three, doesn't matter.

[00:13:11] Rajeeva: So, so it's a question of calling for proposal. The awareness that such a thing is needed, okay? And it's a combination of uh maths, computer science and awareness about cryptography. Okay?

[00:13:11] Rajeeva: Um, that could be one or they could just because eventually it needs to be vetted again by crypto experts. They could uh in India, there is a there is a society called Cryptology Society of India, CRSI. Okay?

[00:13:41] Rajeeva: Uh, we have been having uh annual conferences uh for last 25 years. Okay, every year. In fact, right now, if I didn't come here, I was to go for a crypto conference which is holding in uh I think uh Orissa. At this time only.

[00:13:41] Rajeeva: Last year I attended Indocrypt and then this year I've come here. So, one of the government entities, if they show willingness, they can just hand it over to the cryptological society, CRS said, uh to uh make a proposal and so on.

[00:14:26] Rajeeva: And even a more interesting idea has occurred. There are some approved, internationally approved algorithms of cryptography. Okay? Uh, and uh, early parts it was uh only the US uh government entity approving it.

[00:14:26] Rajeeva: And the cryptography, the joke was among the crypto expert, the joke was when they are able to break it, they they they endorse it. They say it is very good because now nobody else can break it, but they can because they have worked on it.

[00:15:02] Rajeeva: That was a joke and we don't know it is true or not, but but around 2000, so like going back 25 years ago, a little before that it started, the international cryptology society set out a call for proposals that uh new uh advanced encryption standard, AES. Okay?

[00:15:26] Rajeeva: They call for proposals uh and uh out of the proposals the experts chose some maybe 20 or something like that, held a first conference that all these 20 had to come and present and like a question and answer session, others could question them, why this, why not this, etc.

[00:15:46] Rajeeva: And based on that amongst the entire group of experts, they picked five. Those five uh then they called for a year, a year long that everybody could try to analyze and work out and see which one is better, which is weaknesses, can it be broken? Can that be happen etc. and held one more uh year conference, year long.

[00:16:09] Rajeeva: And at the end of that they chose a winner. And uh they the uh uh proposal from Belgium uh was accepted uh as advanced encryption standard and that is in vogue now. Uh the one interesting thing was that uh one of the conditions was that anybody can submit a proposal, but they had to commit that if their algorithm is chosen as the best one and becomes AES, they have to write off all rights on it.

[00:16:42] Rajeeva: They will not get any money. Okay? It is public. It's okay, open source.

[00:16:42] Rajeeva: That was a requirement. And therefore AES is open source. Not just the algorithm, but its entire code is available, algorithm, mathematical it is available, people can say more efficient implementation of AES and so on, so forth.

[00:17:04] Rajeeva: So, what it occurred to me was that uh again, uh either a government entity or even a corporate, because money required will be minimal. Uh, can announce uh call for proposal that anybody can submit a thing for uh UV dat. Uh of course, for it eventually to get thing, the corporate uh Ministry of Corporate Affairs has to be taken in confidence, but that should not be a problem. Okay?

[00:17:36] Rajeeva: So either a government entity or a corporate entity or CSR money of a corporate, uh they don't have to announce any award. Okay? Or some award. Even the name that such and such person's thing became the uh this on electronic voting standard would be great.

[00:17:36] Rajeeva: Some money will be of good but not that that need not be the prime thing.

[00:18:08] Rajeeva: But at the same time they have to get this that they will they will be no uh uh uh no rights. They will it will be open source the winner one. In fact for AES, not only various people had signed up saying that whether it is selected as winner or not, we are making it public.

[00:18:28] Atibhi Sharma: So why is that a requirement? Why is making it public a requirement?

Open source requirements and benefits

[00:18:32] Rajeeva: For something that the corporates will be using, isn't it a...

[00:18:35] Rajeeva: No, see that Well, see it works both ways. See for let let's go back to the mobile phone era in India, okay? Uh, you are too young, you won't know when they were introduced. You know what was the charges?

[00:18:35] Rajeeva: In India, mobile?

[00:18:53] Rajeeva: Uh, go back only 30 years, okay? It was uh 16 rupees per minute incoming and outgoing. You receive a call also, your money is going to go from your pocket. Okay?

[00:18:53] Rajeeva: 16 rupees. And it came down a little, came down a little and Reliance came and just broke the window. And they said it's the they they they they said that it was like Dhirubhai's dream that uh the cost of a postcard was 10 rupees so a call should not cost more than 10 10 paise.

[00:19:28] Rajeeva: So the cost should not call more than 10 paise per minute. And everybody said, are they mad? How can they run a business with that? Okay?

[00:19:28] Rajeeva: And uh the big story there, but actually all the companies which existed and were crying foul against uh Reliance, they themselves gained a lot, Airtel. Because the volumes went up. Okay? Volumes went up and uh that just has changed the all of you would be very surprised to hear these prices, right, today?

[00:20:00] Rajeeva: A call doesn't cost anything. You know, just a monthly fee and that's it. So, so the point is AES, the the the creators uh the two Belgian professors, they became big crypto experts across the globe. They both have come to to India and attended one of our indocrypt conferences.

[00:20:21] Rajeeva: In fact our very first conference, the the the losing finalist author was there and he explained this entire process and without very openly and uh he said that we all went through this, etc, etc. The only thing in the end he said was also that the best may not always win. That is the only line he said.

[00:20:47] Rajeeva: It was very impressive. He was very positive about the whole thing. And uh he says, no wonder the chosen one is very good. Of course, in my view, mind was better, but things like that.

[00:20:47] Rajeeva: So, uh but the uh both of them are big wigs today, crypto world, okay? So the uh you see, the only the after all, the who will be doing these algorithms?

[00:21:11] Rajeeva: It is not the people who are already in the corporate world. It will be academics with crypto background and math background, etc. And this one will drive them equally. So, so instead of see, once there are rights, then who uses which one?

[00:21:11] Rajeeva: So suppose there are four things, then which has and then anybody in using that, they have to give a right and that becomes more complex.

[00:21:35] Rajeeva: And okay? So if at all, uh the entities if let's say CSR money, you give some very good amount to the whoever wins and it could be an international one, it doesn't have to be restricted to only India because basically what you need to do is to write down the rules. What what is it that you want? Okay?

[00:21:35] Rajeeva: And then uh then it is, you make an open thing. Once it is open, it will kind of uh the it will be a big boost for the India as a whole and Indian digital hold, okay?

[00:22:09] Rajeeva: So, uh as it is, people who are in it know it, but So, so I I think it's a win-win for everybody involved and the so if I let's say what are the costs involved? Okay. So the cost would be one is uh let's say if there an award is to be given, not a must, but good to have some token token or heavy or whatever. That's up to.

[00:22:35] Rajeeva: The only other thing will be uh holding holding three conferences uh early. Right. Advertisement you don't have to do, it's a electronic everything. So uh no other cost.

[00:22:35] Rajeeva: And uh the the uh original thing writing maybe CRSI could be funded a little and uh the Cryptology Society India and some of us uh we could work on that and write down a the main thing is that your original call has to be properly written.

[00:23:05] Rajeeva: Without that things will not work. So that has to be written well. So the total cost involved is not much, but the big win is there. Uh getting the digital framework that bringing India as it is people know, but bringing it to forefront that yeah, India analysis that because this is a uh even in a uh I mean for example, at CMI, we have a lot of uh visitors coming from uh European and US and so on.

[00:23:40] Rajeeva: And we have a big tie up with uh CNRS, the French academy, okay? And uh so so so let's say even in their governing board, uh they have to vote. Now, it is known that if you have to vote publicly, whoever is in favor, raise your hand versus you just write it secretly and then share and do uh the votes can be different.

[00:24:07] Rajeeva: And they had been they have been trying around by uh this electronic, but it it's a same problem that how do you verify that uh what you are getting totals is the correct one. So there are multiple applications, okay? And uh so I would like to propose that, but we'll see.

Cryptography applications beyond voting

[00:24:35] Atibhi Sharma: Very exciting. This is new. I think we haven't done this much in any other field. Has cryptography even been adopted anywhere else in India?

[00:24:35] Atibhi Sharma: Any other...

[00:24:44] Atibhi Sharma: Except for the voting part?

[00:24:46] Rajeeva: No, no. Cryptography, the primary need of cryptography is actually defense. Right. Okay.

[00:24:51] Rajeeva: Okay? It's origin is with defense.

[00:24:54] Atibhi Sharma: We're adopting it to a different...

[00:24:56] Atibhi Sharma: The course that we're adopting it.

[00:24:57] Rajeeva: No, it has been adopted elsewhere like in the voting. But the origin is of course uh the defense. Now it has been adopted with uh in the banking system, the the how do we transfer money? The OTP etc is a the requirement is different but the purpose purpose is the building block is that.

[00:25:21] Rajeeva: In fact, uh you would have heard anybody who is use and now everybody because of lockdown, everybody has had to use uh uh electronic transfer of money and all that. So banks tell tell you that do not uh go to just HTTP. You have to go to HTTPS. So what is the difference?

[00:25:41] Atibhi Sharma: The security.

[00:25:42] Rajeeva: The difference is cryptography. That if somebody is snooping on the entire communication between your computer and the bank's uh computer, server, uh they will still not be able to make head or tail of what you have done. Because if they can, they can spoof you and instead of transferring 1,000, they can transfer 1 lakh. Right?

[00:26:03] Rajeeva: So, so cryptography is at the core without that, the electronic expansion would not have happened. Okay? So it is there. It started with defense, then it's then moved to banking, then to elections.

[00:26:03] Rajeeva: And now we can go to even other, it's not just general elections, but we can put it to the corporate world and uh in place of paper ballot or absentee ballot as it is called, we move it to this way.

[00:26:33] Atibhi Sharma: This is very exciting. Thank you. Thank you so much for your time today.

[00:26:37] Rajeeva: Thank you.

[00:26:38] Atibhi Sharma: Thank you.

References

[1] Miles E. Smid. Development of the Advanced Encryption Standard. *Journal of Research of the National Institute of Standards and Technology*, 126:126024, 2021. doi:10.6028/jres.126.024.