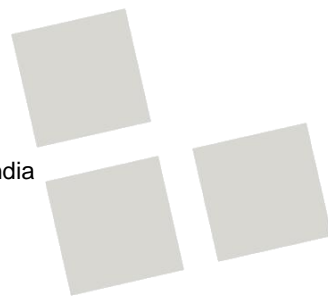


Corpus Enterprises Private Limited

Wework Rajapushpa Summit,
Nanakramguda, Financial District. Hyderabad – 500032, Telangana, India
CIN: U85110KA1999PTC024766



To,
Sh. Anil Kumar Bhardwaj,
Advisor (B&CS)
Telecom Regulatory Authority of India.

Reference: Consultation Paper No.12/2022.

Subject: Our recommendations and detailed response on issues related to Draft Regulations 2022 raised in this CP. We have provided valid reasons and Justifications and have included annexures to support the recommendations.

Dear Sir,

We are Corpus Enterprises Private Limited an IPTV Technology Company. Our platform is in use by several services providers in India including Andhra Pradesh Fibernet and has passed the technical Audit conducted by Broadcasters and TRAI panel Auditors and BECIL. We provide end to end IPTV solutions including Content security (DRM), Streaming and compression technologies.

Our customers have completed the RIO agreements with major broadcasters as per the list below

1. Star India Private Ltd
2. Zee Entertainment Enterprises Ltd
3. Sony Pictures Networks India Private Ltd
4. Indiacast Media Private Ltd -
5. Indiacast Media Private Ltd – Warner
6. Gemini TV Distribution Services Private Ltd
7. Eenadu Television Private Ltd
8. Bennet Coleman & Company Ltd
9. T.V.Today Network Limited
10. New Delhi Television Ltd
11. Discovery Communication India
12. Epic Television Networks Private Ltd

We are submitting our response to the consultation paper issued on 9th September 2022 as per the prescribed format. Detailed explanations and justification for our responses for some of the Clauses were submitted in Annexures.

(E) DRM Requirements for conditional access by subscribers and encryption for IPTV services

Sl. No.	Proposed DRM Requirements for conditional access by subscribers and encryption	Do you agree with the Draft Regulations proposed in this CP (Yes/No)	If you do not agree with the amendment proposed in this CP, then provide amended Clause proposed by you	Reasons with full justification for your response
1	DPO shall ensure that the current version of the DRM in use do not have any history of hacking. A written declaration from the DRM vendor shall be required to be furnished on an annual basis as compliance of this requirement.	Yes		
2	DRM shall ensure all logs are un-editable, stamped with date and time of all transactions (all activations, deactivation, channel authorization/assignment and unauthorization / de-assignments and change in MAC ID/STB). The DRM shall not allow altering or modification of any logs. There shall be no facility for the distributor/users to purge logs.	Yes		

3	<p>DRM deployed do not have facility to activate and deactivate a Set Top Box (STB) directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs shall be done with the commands of the SMS integrated with DRM. The DRM shall be integrated with the SMS in a manner that ensures security of the channel.</p>	Yes		
4	<p>The SMS and the DRM should be integrated in such manner that activation and deactivation of STB happen simultaneously in both the systems. Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the DRM.</p>	Yes		
5	<p>DRM deployed should be able to support two-way networks only.</p>	Yes		

6		The DRM deployed should be able to support both carded as well as card-less STBs for any provisioning.	No	The DRM deployed should be able to support both carded card-less STBs & Smart TV for any provisioning.	DRM encryption + the traditional FP mechanism + HTTPS secured unicast delivery + private network + authentication & authorization access will add up multiple layers of content security. Card less solution will ensure interoperability between providers allowing subscribers to switch over seamlessly Allowing DRM supported smart TV's will save the cost for the subscriber. More details in Annexure 1
7		The DRM deployed should be able to generate, record, maintain independent reports and logs for verification purpose during audits corresponding to each command executed in the DRM issued by the SMS integrated with the DRM for last two (2) years minimum. The reports must have date and time stamp. Proposed reports should include:	Yes		

(a)	Unique active STB count as well as MAC ID wise on any desirable date	Yes		
(b)	Unique bouquet/channel active for a specific STB on any desirable date	Yes		
(c)	MAC ID wise activation-deactivation report for service requests	Yes		
(d)	Any alteration in bouquet and/or channels configured in DRM	Yes		
(e)	Blacklist STB report	Yes		
(f)	Product code pertaining to channels/ bouquets available on the platform	Yes		
(g)	Channel/bouquet authorization/assignment to STB along with start date and end date of entitlement	Yes		
(h)	STB-VC pairing / de-pairing (if applicable)	Yes		
(i)	STB activation / de-activation	Yes		
(j)	Channels assignment to STB	Yes		
(k)	Report of the activations or the deactivations of a particular channel for a given period	Yes		
(l)	The total number of registered subscribers	Yes		
(m)	The total number of active subscribers	Yes		
(n)	The total number of temporary suspended subscribers	Yes		
(o)	The total number of deactivated subscribers	Yes		
(p)	List of blacklisted STBs in the DRM	Yes		

	(q)	Channel and bouquet wise monthly subscription report in the prescribed format.	Yes		
	(r)	The names of the channels forming part of each bouquet	Yes		
	(s)	The total number of active subscribers subscribing to a particular channel or bouquet at a given time	Yes		
	(t)	The name of a-la carte channel and bouquet subscribed by a subscriber	Yes		
	(u)	The ageing report for subscription of a particular channel or bouquet	Yes		
8		DRM deployed should be able to tag and blacklist the STB independently in case of any piracy.	Yes		
9		DRM deployed should have the technical capability in India to maintain the systems on 24x7 basis throughout the year.	Yes		
10		The DRM and SMS should be integrated in such manner that upon deactivation of any subscriber from the SMS, all program/services shall be denied to that subscriber.	Yes		

11	The DRM should be capable of generating, recording and preserving unedited data / logs for at least two consecutive years for each command executed through the DRM, including logs of each command of the SMS integrated with the DRM.	Yes		
12	DRM deployed should be capable to support both software base as well as hardware base security.	Yes		
13	DRM shall not support carriage of channel with same name or nomenclature in the distributor's network served by each headend under more than one LCN, and another channel descriptor. Further, each channel available in DRM shall be uniquely mapped with channels available in SMS.	Yes		
14	DRM shall be capable of adding/modifying channels/bouquets as may be required on real time basis in line with the activity performed in SMS.	Yes		
15	DRM should support only agreed DPO's branded/proprietary and DPO's supplied business model for STBs	Yes		
16	When infrastructure sharing is available, in such cases DRM shall be	Yes		

		capable to support multiple DPOs.			
17		DRM should support content protection and usage rules enforcement for B2C model	Yes		
18		DRM should be capable of handling at least 3 million license transactions per minute.	Yes		
19		DRM should support encryption of individual tracks of a content stream with individual keys, i.e., track level protection	Yes		
20		DRM should support key rotation, i.e., periodic changing of security keys	Yes		

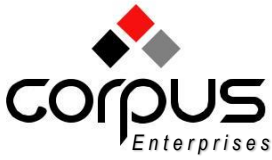
21		<p>In case DPO has deployed hybrid STBs, DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs.</p>	No	<p>Hybrid STB is an STB with access to internet as well as Linear services. DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system. DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs. DPO is free to integrate the OTT content on the UI along with linear content at his disposal. The OTT content has to be protected by OTT vendor by means of DRM and CPE certification.</p>	<p>DPO should be allowed to provide a single device and single interface to use both the Linear services and OTT content for the consumer convenience and cost benefit. The OTT content will be accesible only from the the resident OTT application anyway and the STB is merely presenting the matadata of the OTT app as a promotion. THE DPO DRM has no role whatsoever with the OTT content access or vice-versa.</p>
22		<p>There shall not be any active unique subscriber outside the database tables. Further, there shall not be an option to split DRM database for creation of more than one instance by a DPO or a vendor.</p>	Yes		

23		It must support the following options with reference to uploading of unique access (UA)/MAC ID details in DRM database:	Yes		
	(a)	A secure un-editable file of MAC ID details, as purchased by the distributor, to be uploaded by the DRM vendor on the DRM server directly,	Yes		
	(b)	If it is uploaded in any other form, UA/MAC ID in DRM database shall be captured in logs,	Yes		
	(c)	Further, DRM shall support an automated, application programming interface (API)-based mechanism to populate such UA/MAC ID details in the SMS, without any manual intervention.	Yes		
24		It shall be mandatory to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers:	Yes		
		Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server:	Yes		

		Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB UA/MAC ID details, entitlement level information, etc	Yes		
25		DRM and SMS shall ensure that the access to database is available to authorized users only, and in “read only” mode only. Further, the database audit trail shall be permanently enabled.	Yes		
		Explanation: Database here refers to the database where data and log of all activities related to STB activation, deactivation, subscription data, STB UA/MAC ID details, entitlement level information, etc., is being stored.	Yes		
26		Provision of à-la-carte channels or bouquet:	Yes		
	(a)	DRM (and SMS) shall be able to handle all the channels, made available on a platform, in à la carte mode.	Yes		
	(b)	DRM (and SMS) shall have the capability to handle such number of broadcaster/DPO bouquets, as required by the DPO.	Yes		
27		DRM and SMS applications, along with their respective databases, shall be stored in such a way that	Yes		

		they can be separately identified.			
28		DRM shall have a provision to export the database/report for reconciliation with the SMS database. Further, there shall be a provision of reconciliation through secure APIs/secure scripts.	Yes		
29		DRM should have the following features:			
	(a)	The entitlement end date in DRM shall be equal to the entitlement end date in SMS,	Yes		
	(b)	The entitlement end date in DRM shall be open and SMS shall manage entitlements based on the billing cycles and payments.	Yes		
30		There shall be unique license key required for viewing every 10 minutes in DRM deployed by DPO.	Yes		
31		For every change in channels, fresh license keys should be issued by the DRM. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB from any other source other than the one specified by the IPTV system.	Yes		

32	DRM servers should comply with extant Rules and Regulations including relevant clause under extant provisions (if any) relating to data localisation, data security and privacy. It should not be allowed to connect main DRM server to some other location (India or other country) with some proxy or another server to integrate with SMS and DPO system.	Yes		
33	IPTV transmission has to be in multicast mode only just like cable TV transmission. There cannot be any such case where unicast is allowed. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device.	No	IPTV transmission is to be restricted to the private network of the DPO/LCO in either multicast/unicast format, IPTV should not be available/transmitted over the Internet. In case of unicast delivery the DPO has to use HTTPS along with TLS for secure point to point delivery of the content stream. The DPO can engage with Telco's for long distance transmission over a dedicated leased line or through a TLS encrypted tunnel in case of shared infrastructure. STBs with facilities for recording programs shall have a copy protection system	Multicast is less secure than the unicast. Multicast management in the last mile is costly and highly technical for the LCO to handle. Unicast in conjunction with HTTPS and TLS is already employed for banking systems also for financial transactions with highest grade of security. Unicast on the otherhand is already being used for all broadband communications and the LCO last mile is managing it. DPO should be allowed to use dedicated secured/telco links for cost



Corpus Enterprises Private Limited

Wework Rajapushpa Summit,
Nanakramguda, Financial District. Hyderabad – 500032, Telangana, India
CIN: U85110KA1999PTC024766

				(i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device.	effective long distance transmission.DRM encryption along with the traditional features of FP has to address the security of the linear content. More details in Annexure 1.
--	--	--	--	---	--

34		IPTV transmission should not be allowed to configure any content delivery network (CDN) in their system to deliver linear content to STBs.	No	only private CDN's can be used by the DPO and no public CDN is allowed. Private CDN nodes can only be accessed by the DPO customer base and should not be accesible from any other network.	CDN's do not breach security, they merely serve the purpose of stream multiplication at the last miles similar to EDFA or edge QAM in traditional CaTV. The content is secured by the DRM and the key exchange is carried out-of-band over a secured point to point connection, denying any man in the middle attack, CDN's are already used worldwide by all content providers proving that the security is not at stake. CDN's will save the long distance transmission cost/bandwidth for the DPO, will help the DPO to enhance the QoE for end user. CDN's will also prepare the DPO to deliver 4K in future based on CPE. More details in Annexure 2
----	--	--	----	---	---

35		IPTV should not be allowed to deliver linear content to any other device except STB which has been whitelisted in DRM.	No	IPTV should be allowed to deliver linear content to any large screen devices like smart TV's & STB which has been integrated and declared to be tested with the DRM security.	DRM security + the traditional FP mechanism + HTTPS secured unicast delivery + private network access together add up multiple layers of content security. Consumer has to get the cost benefit from a smart TV. Also this will ensure interoperability for the end consumer to choose from different providers Please refer to Annexure 3
36		IPTV should have capability to implement session based/token authentication with token authentication duration to be controllable to few minutes.	Yes		
37		IPTV system should not allow recording of linear channel at headend/network level. It should be allowed to be recorded at STB/DVR level only, without there being any option available to transfer such recorded content to any other device.	Yes		

38		The DRM should have following policies implemented:			
	(a)	It should restrict user to editing or saving content in part or full.	Yes		
	(b)	It should restrict user from sharing or forwarding or mirroring the content from the STB	Yes		
	(c)	It should disallow user to take screen shots or screen grabs or screenrecording.	Yes		
	(d)	It should lock access to authorized STBs only.	No	It should lock access to authorized STB and smart TV only.	DRM security + the traditional FP mechanism + HTTPS secured unicast delivery + private network access together add up multiple layers of content security. Consumer has to get the cost benefit from a smart TV. Also this will ensure interoperability for the end consumer to choose from different providers
	(e)	It should have Geo blocking, that enables a broadcaster to determine and instruct the DPO/IPTV service provider to restrict the broadcast of TV channels in locations.	Yes		

	(f)	It should be able to set expiry date to recorded content at STB end based on various policies.	Yes		
39		The DRM should have the capability of being upgraded over-the-air (OTA) so that the connected STBs always have the most upgraded version of the DRM.	Yes		
40		The DPO shall ensure that the DRM is updated/upgraded at regular intervals by installing necessary patches, error corrections, additions, version releases, etc. so as to ensure protection of channels and content at all times	Yes		

41	<p>No such functionality should be added to or removed from the DRM which compromises security of channels. DPO shall be responsible for encryption of channels' signals before their transmission through its IPTV platform using DRM integrated STBs. All costs / expenses (by whatever name called) that are required to be incurred or become payable for such upgradation and for retransmission and/or delivery/distribution of channels to subscribers shall be borne solely by such DPO. The DPO shall employ all reasonable security systems and procedures to prevent any loss, theft, piracy, unauthorized use, reception or copying of channels or any part thereof and shall notify broadcasters as soon as practicable after it becomes aware that such an event has occurred</p>	Yes		
42	<p>The DRM should not in any way interfere with / invalidate fingerprinting.</p>	Yes		
43	<p>DPO shall promptly, and at it sole cost and expense, correct any issues with the DRM (such as bugs, defects, omissions or the like) that prevents subscribers from accessing the DRM integrated STBs or</p>	Yes		

		channels through the DRM integrated STBs			
44		DPO shall provide broadcasters with video and audio codecs supported by the DRM integrated STBs. The DPO shall ensure that no such changes/modifications are made to such codecs parameters that will require broadcasters to incur any expense for delivery of channels / content that are free from viewer discernible problems (including, without limitation, video with no audio, audio with no video or significant signal distortion	Yes		

45	DRM should ensure that the integrated STBs are verifiably located within India by reference to internet protocol address and service address. Further, the DRM shall not permit delivery to an Internet/mobile device. The DRM must use industry standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.	No	DRM should ensure that the integrated STBs and Smart TVs are verifiably located within India by reference to internet protocol address and service address. The DRM must use industry standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.	Internet access is required for the client devices to access the DRM key servers, reporting the IP addressing and geo-location etc.. Implementation of DRM + FP + Secure HTTPS unicast + Private IP address will ensure the stream integrity and security. More details in Annexure 1.
46	DRM should ensure that channels are accessible on integrated STBs of only such subscribers who are then-current, valid subscribers of the distributor of channels, and such confirmation must take place prior to the DRM actually delivering (or authorizing the delivery of) channel to the integrated STBs of such subscribers.	No	DRM should ensure that channels are accessible on DRM certified STB and SMART TV of only such subscribers who are then-current, valid subscribers of the distributor of channels. Authorization to the content access should be implemented at both middleware and DRM levels.	Stream request for un-authorized content can be prohibited from the DPO STB or smart TV, the DRM can also authorize at the next level for subscription in synchronization with the SMS.
47	Upon deactivation of any subscriber from the SMS, the DRM shall restrict delivery of all programme/services to that subscriber.	Yes		

48		The DRM shall not allow insertion of any self-promotion and/or any third party and/or paid for advertisements (including banners and aston bands) before, during or after transmission of linear channels.	Yes		
49		The DRM shall not permit subscribers to record and/or store channels/content from channels.	No	IPTV system should not allow recording of linear channel at headend/network level. It should be allowed to be recorded at STB/DVR level only, without there being any option available to transfer such recorded content to any other device.	Its already addresses in clause 37
50		The DRM should not mask/remove any copyright, trademark or any other proprietary information on the channels at the time of their retransmission.	Yes		
51		The DPO shall not sublicense the DRM and/or any rights granted to the DPO by the broadcaster to any entity for re-transmission of channels to subscribers	Yes		

Annexure – 1:

Reference to Recommendation 33: IPTV transmission has to be in multicast mode only just like cable TV transmission. There cannot be any such case where unicast is allowed.

Unicast delivery security with HTTPS with TLS - <https://datatracker.ietf.org/doc/html/rfc8446>

IEEE publication on multicast delivery –

Unicast is the latest technology and has higher benefits to service providers than Multicast. Encrypted unicast streaming is already followed in industry and should be allowed to stream linear TV services. Operators should be allowed to use latest technology without compromising content security. We have listed few benefits of Unicast streaming here over multicast.

Unicast streaming is over TCP, which is a connection-oriented protocol. Source-to-receiver connection issues can be traced and resolved easily. TCP has a built-in error detection and correction mechanism to guarantee stream delivery to the receiver.

Security of Content on Unicast

Unicast content is secured by a DRM using the **latest AES-128/256-bit encryption**. Authorization for content viewing can be adaptive to the market demand by rules like several views/time of the day etc... The transport layer is secured using TLS, which will enhance the security further. The TLS and AES-128/256 are mandated by RBI, SEBI, and DSCI (Data Security Council of India) and are used to secure financial transactions worldwide. The CPE devices can be identified using the DRM libraries on them. In case of content theft/piracy, DRM is capable of invoking commands (similar to CAS) to identify the erring subscriber device. Closed network transmission can be ensured by using private IP addresses.

Prevent Delivery of content to IP addresses outside of India or to Proxies

Private CDNs operating with private IP addresses (cannot connect over the internet) adhering to the above security protocols should be allowed for intra-network streaming. This will help the operator to stream secure ABR content to the subscriber STB. The CDN will mitigate the issue of clogging a central point of the network and allow the operator to scale steadily. The CDN cannot be a security loophole as the content is already secured with DRM. The communication between the DRM server and an authorized client is secured by Authentication, authorization and TLS certification and the key exchange is out-of-band with respect to the video stream and does not involve the CDN.

Transmission Reliability to Last Mile unmanaged Network

A Multicast is a bad option for the last-mile network (a network connecting the end subscribers) that is typically unmanaged. Multicast is treated as broadcast traffic in many of the legacy devices, broadcast traffic overwhelms the network with unnecessary traffic loops and chokes the network and thus denies service to the end subscriber.

Unicast traffic is source-to-receiver traffic only and the network traffic is generated only upon the receiver request, unlike multicast, which does not create broadcast traffic loops. Unicast is best suited for any last-mile model, thus ensuring service delivery in all kinds of networks.

IEEE publication on multicast delivery –

<https://ieeexplore.ieee.org/abstract/document/819174>

Quality of service

Multicast streams or not viable for multibit-rate transmission due to its inherent, UDP, connectionless transmission. So the quality of the stream has to be unique for all kinds of devices

and networks irrespective of the end subscribers viewing device capability or the quality or capacity of the subscriber network.

Unicast can comprise ABR (adaptive bit-rate) streaming optionally, which can deliver different qualities of the same content, efficiently, based on different viewing devices' capabilities or based on the quality or capacity of the subscriber network. The stream can adapt automatically to a different bit rate/quality based on the network/device capabilities.

Cost

Multicast is suited for a managed network like GPON only. The cost of upgrading the existing network designed for broadband-only is prohibitive as the RoI does not start immediately. The need to upgrade the networks that were designed for broadband-only is immediate in the case of multicast. Unicast is suited for all networks, unlike multicast. The need to upgrade to a completely managed network and hence the cost is not immediate. It can happen linearly in a phased manner based on subscription and RoI.

Annexure – 2: How operator can leverage Private CDN (within private network) to deliver linear TV services

Reference to Recommendation no.34: IPTV transmission should not be allowed to configure any content delivery network (CDN) in their system to deliver linear content to STBs.

IEEE publication on CDN security orchestration –

<https://ieeexplore.ieee.org/abstract/document/8459910>

Private IP addresses are not routable over the internet -

<https://datatracker.ietf.org/doc/html/rfc1918>

Private CDNs operating with private IP addresses (cannot connect over the internet) adhering to the above security protocols should be allowed for intra-network streaming. This will help the operator to stream secure ABR content to the subscriber STB. The CDN will mitigate the issue of clogging a central point of the network and allow the operator to scale steadily. The CDN cannot be a security loophole as the content is already secured with DRM. The communication between the DRM server and an authorized client is secured by Authentication, authorization and TLS certification and the key exchange is out-of-band with respect to the video stream and does not involve the CDN.

Annexure – 3: Why Smart TV should be considered along with STB for delivery of linear content

Reference to Recommendation clause35: IPTV should not be allowed to deliver linear content to any other device except STB which has been whitelisted in DRM.

Smart TV penetration has increased over the past few years in India and is growing phenomenally. The Smart TV in house has capabilities of receiving DRM encrypted content over home network. DRM on Smart TV Should supports:

- Finger Printing
- OSD
- Water Marking
- Encryption / Decryption

The operators offering broadband connection to the house can deliver IPTV services on their network to the TVs. The customer has the choice of choosing the network and the device STB or Smart TV to view contents. This allows much needed interoperability Also the Smart TV is fixed device similar to Set top Box. Hence we recommend that the network provider should be allowed to deliver services to the connected Smart TV along with the Set top Box.

RFC and IEEE reference –

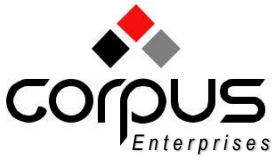
Private IP addresses are not routable over the internet -

<https://datatracker.ietf.org/doc/html/rfc1918>

Unicast delivery security with HTTPS with TLS - <https://datatracker.ietf.org/doc/html/rfc8446>

IEEE publication on multicast delivery –

<https://ieeexplore.ieee.org/abstract/document/819174>



Corpus Enterprises Private Limited

Wework Rajapushpa Summit,
Nanakramguda, Financial District. Hyderabad – 500032, Telangana, India
CIN: U85110KA1999PTC024766

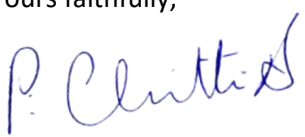

IEEE publication on CDN security orchestration –

<https://ieeexplore.ieee.org/abstract/document/8459910>

Thanking you,

For Corpus Enterprises Pvt Ltd

Yours faithfully,

Chittibabu Pothana

AVP, Business Development