International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

A Secured Video Conferencing System Architecture using A Hybrid of Two Homomorphic Encryption Schemes: A Case of Zoom

Arnold Mashud Abukari[1], Edem Kwedzo Bankas[2] and Mohammed Muniru Iddrisu[3]
[1]Ph.D., Student, Department of Computer Science, Tamale Technical University, Ghana.
[2]Senior Lecturer, Department of Computer Science, University for Development Studies, Ghana.
[3]Associate Professor, Department of Mathematics, University for Development, Ghana.

***Abstract*:- The Coronavirus Disease (COVID-19) Pandemic has promoted the increasing patronage of video conferencing solutions like Zoom globally as the only way organisations, Governmental agencies and individuals can continue to conduct meetings and other teleworking activities to control the spread of COVID-19. Zoom came under serious security scrutiny after reports of Zoombombing, confidentiality issues and the alleged routing zoom calls through the servers of China. Even though Zoom uses 256-bit TLS and AES-256 Encryption schemes, it failed to address the security concerns expressed by researchers and users. In an attempt to find solution to these security concerns, we have proposed a new system architecture that allows the user or an organisation to take responsibility of securing the video and audio files generated using the zoom conferencing solution.**

Keywords: Video Conferencing, Zoom, COVID-19, Cloud, Homomorphic Encryption, data communication

I. INTRODUCTION

The ability to establish a live connection between people at different geographical locations for the purposes of communication using audio-visual devices is referred to as Video Conferencing (Rop and Bett, 2012). The transmission of motion videos and sounds and for that matter multimedia across many geographical locations provides an enabling environment for teleworking and virtual meetings to be held (ITU-T,2003). The communication is done as if the connected parties were in the same room. It must be noted that, teleworking and videoconferencing has been with us for long. Video conferencing has become an interesting research area in the wake of the COVID-19 Pandemic that has confronted the world. Government agencies and businesses and educational institutions across the world have adopted the concept of Teleworking and video conferencing as the major alternatives to continue driving the economies and getting work done. Virtual meetings using the video conferencing technologies have been adopted and implemented across Governments and businesses to enable a synchronous participation of teleworkers in geographically dispersed locations. Despite the widespread adoption, there has been several reportage regarding the security and privacy of users using video conferencing application for communications (Wakefield, 2020). Cloud-based video conferencing applications like Zoom has been in the media for discussion over security concerns during this COVID-19 era. Zoom bombing, Privacy concerns regarding using video chats online and the alleged routing of video chats through the servers of China were some of the serious security concerns raised by users across the globe (Whittaker, 2020). These security concerns identified in Zoom video conferencing application has lead to researchers developing interest in the security policy of Zoom and the transmission of the meeting encryption keys through Chinese servers. (Bill and John, 2020) examined the encryption that protects meetings in Zoom teleconference application and reveals that the Video Conferencing giants had rolled out their own encryption scheme which they described as having significant weaknesses. Contrary to the Advanced Encryption Scheme – 256 (AES-256) encryption for communication data as claimed by Zoom, (Bill and John, 2020) observed that both audio and video streams were all encrypted by AES-128 encryption schemes used in Electronic Code Book (ECB) mode. (Bill and John, 2020) further argues that patterns present in plaintext are preserved during encryption with AES-128 used in ECB mode and hence not recommended. The AES-128 packets are generated by Zoom servers but in some cases are delivered to Zoom meeting participants through servers in China (Bill and John, 2020). These research findings lead to some Government Agencies, Giant companies like Google and businesses warning their employees not to use Zoom video conferencing application for their meetings (Statt, 2020). Zoom video conferencing application came under attack compelling their Chief Executive officer, Eric Yuan to publicly apologise and promise to fix the security issues identified but however said the routing through the servers of China was a mistake (Wakefield, 2020).

II. VIDEO CONFERENCING CHALLENGES

Video Conferencing users over the years have debated on the challenges the adoption of video conferencing comes with as against the benefits they derive for their respective companies. One of the major challenges confronting organisations, businesses and Government Agencies from adopting video conferencing technology is security (Honeyman et al, 1998). The fear of video conversation being intercepted via the internet affected the usage and

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

adoption of video conferencing applications prior to the emergence of the Coronavirus Disease (COVID-19). Encrypting,the transmission of the data, and the user confidentially were crucial in providing security for video conferencing applications. "Whether the systems or communication sessions are hosted on secure or non-secure networks, the security threats and concerns are fundamentally the same." (Rop and Bett, 2012) argues. (Singh, 2006) identified some security and key mechanisms that needs attention to address the video conferencing security in order to prevent attacks through eavesdropping, Denial of Service (DoS), tampering with messages, spoofing and repudiation or forgery. With the increasing use of internet infrastructure and internet protocols (IP), there is an increasing demand for security awareness in the use of IP-Based audio, video and exchange of data (Frost and Sullivan,2006). The easiest and simplest way to use a video conferencing solutions is through an open network which is believed to be associated with high risk as argued by (Frost and Sullivan, 2006). To address the security related concerns associated with using an IP-Based data exchange, audio and video solutions, (Rop and Bett, 2012) proposed steps and measures to secure IP-Based video conferencing applications. Endpoint protection, proper firewall configurations, Network Access Traversal (NAT) configurations, the application of dedicated Virtual Private Networks (VPN), Gatekeepers and Multipoint Control Unit(MCU) configurations were the applicable solutions areas according to (Rop and Bett, 2012). Despite the security measures outlined by (Rop and Bett, 2012), notable among their recommendation for the purposes of our research is the use of encryption methods to prevent the unauthorised monitoring of sessions by hackers or malicious internet users.

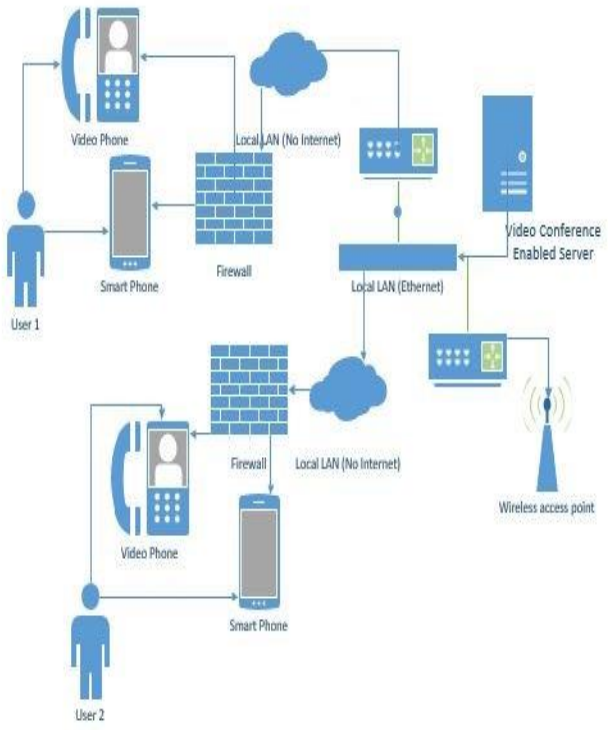

Figure 1: Video conferencing architecture (Lazar, 2019)

III. VIDEO CONFERENCING IN CLOUD

According to a research conducted by Nemertes, a global research-based advisory and consulting firm that analyzes the business value of emerging technologies, about 42.9% of organisations globally have adopted cloud video conferencing (Lazar, 2019). The research further indicates that about 52.2% of Financial Services organisations globally have also adopted the video conferencing applications based in the cloud.

Cloud video conferencing outlined by (Lazar, 2019) makes it easier for any organization to quickly deploy high-quality and feature-rich services. It also saves time for the video conferencing solutions providers meeting spaces without having to invest in large, upfront capital expenditures for both organisations and that of the cloud service providers.

Figure 2: Cloud video conferencing (Lazar, 2019)

IV. ZOOM SECURITY

On April 1, 2020, Obed Gal released the Zoom security details on the Zoom official website in their quest to win back their global confidence in the wake of the security concerns expressed during the Coronavirus Disease (COVID-19) pandemic. In the blog post, Obed Gal said "**To be clear, in a meeting where all of the participants are using Zoom clients, and the meeting is not recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.**" The blog post by Zoom only addressed a situation where the meetings are not recorded but was silent on the security protocols and safeguarding of recorded meetings in the Zoom cloud servers. Even though, Zoom states that in a situation where all participants are using the Zoom applications, they do not have access to the user's content and hence zoom servers and their employees cannot have access to the user's content during the transmission process.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

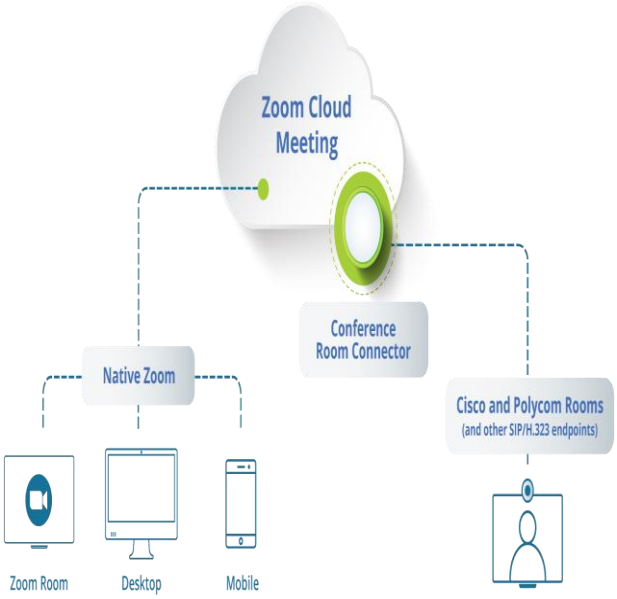

Figure 3: Zoom Architecture (Gal, 2020)

It is however interesting to note that the encryption processes are not done by the Zoom client or Zoom user but rather by Zoom Application either through their Zoom client application or through their servers. Zoom also admitted that their encryption processes are unable to address devices that do not use Zoom communication protocol (Gal, 2020). A situation that further increases our interest to conduct this research.

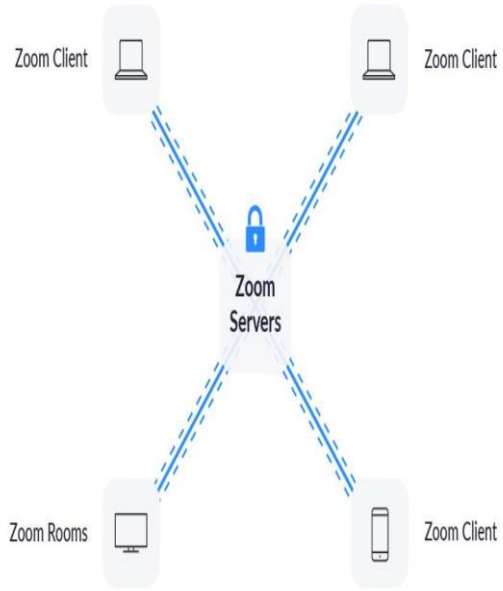

Figure 4: Zoom client – server architecture (Gal, 2020)

The Zoom Cloud video conferencing solution accepts other communication channels like SIP/H.323 room-based systems and Public Switched Telephone Network (PSTN) but providing security for such communication channels either than the proprietary Zoom communication channel is a major concern to researchers and users across the globe since the encryption used to protect users and the transmission of data do not support non-zoom communication channels (Gal, 2020). Despite the security challenges in using non-zoom communication channels, Zoom has developed a mechanism of mitigating this through the use of Zoom connectors. These connectors include telephony connector, conference room connector, Skype for Business connector, Cloud recording connector and live streaming connector.

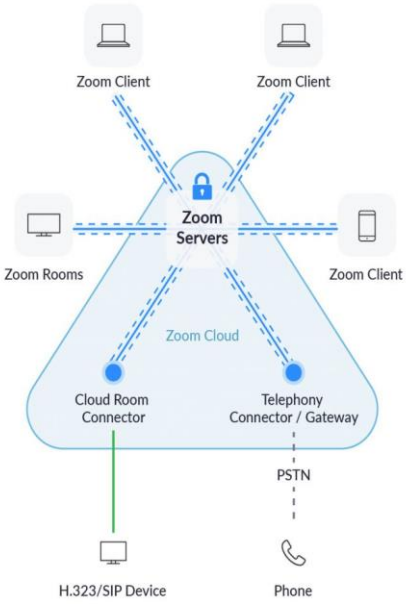

Figure 5: Zoom cloud with connectors (Gal, 2020)

According to the video conferencing giant, Zoom uses 256-bit TLS encryption to protect the communications that are established by Zoom video conferencing application users. The shared contents from the Zoom video conferencing users are secured using the AES-256 Encryption scheme.

IV. PROPOSED SYSTEM ARCHITECTURE

In this research paper, we propose a new architecture that allows the user, government agency or an organisation apply our proposed architecture to help improve security in the entire zoom video conferencing solution. In the proposed solution architecture, a hybrid of two encryption schemes is adopted and implemented at the Zoom video conferencing client's end. The video and audio files are encrypted using a hybrid of the two encryption scheme to generate an encrypted file Enc(Enc d) which is sent via the zoom's 256-bit Transportation layer Security (256-bit TLS) after going through AES-256 encryption in the zoom cloud security encryption scheme.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

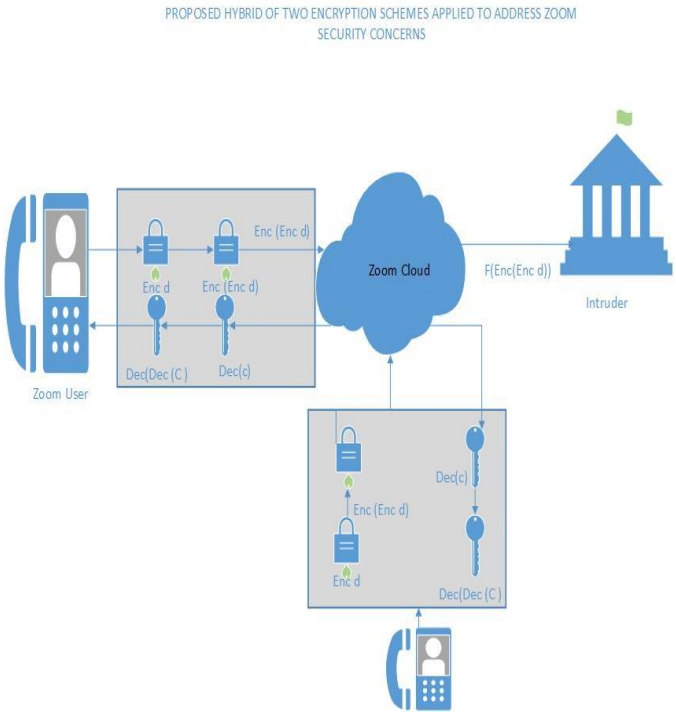

Figure 6: Our proposed Solution Architecture

A. PROPOSED SOLUTION ENCYPTION ALGORITHM

Algorithm 1	**Proposed solution architecture algorithm Decryption**
Input	$d = v + a$, where v and a are video and audio respectively
Output	$f(Enc(Enc\ d))$
Step 1 (First layer)	Encrypt ***d*** to generate $Enc\ (d)$
Step 2(Second layer)	Encrypt $Enc\ (d)$ to generate $Enc(Enc(d))$
Step 3	Send $Enc(Enc(d))$ to Zoom cloud
Step 4	Zoom cloud performs operations to generate $f(Enc(Enc(d)))$ without having access to the video and audio files encrypted by the zoom video conferencing client
Step 5	Zoom routes $f(Enc(Enc(d)))$ to Intruder

B. PROPOSED SOLUTION DECRYPTION ALGORITHM

Algorithm 2	:	**Proposed solution architecture algorithm Encryption**
Input	:	$f(Enc(Enc\ d))$
Output	:	d
Step 1	:	Zoom sends $f(Enc(Enc\ d))$ to Zoom user.
Step 2	:	Decrypt $f(Enc(Enc\ d))$ to generate $Dec\ (d) = Enc(Enc\ (d))$
Step 3	:	Decrypt $Dec(Dec\ (d))$ to generate d.

V. CONCLUSION

In this research paper, we have proposed a new video conferencing architecture using Zoom cloud as a case study. The proposed Architecture allows the Zoom users to implement their own security measures using a hybrid of two homomorphic encryption schemes. Zoom cloud video conferencing solution has come under serious attack after admitting they have mistakenly routed through China's servers during wake of the COVID-19 Pandemic. In our proposed solution architecture we proposed a two layer encryption of two different encryption schemes before sending the encrypted video and audio files through the 256-bit TLS scheme by Zoom Cloud. An implementation of our proposed solution architecture will secure video and audio data generated which can only be decrypted by the zoom user. In the event a conference meeting, video and audio files are being intercepted by other third-party, our architecture when implemented will improve security since the third-party and the Zoom Cloud can only have access to an encrypted version of the video and audio files.

REFERENCES

[1] Bill, M & John, S. (2020). Move fast and roll your own crypto. Retrieved from https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[2] Fouad, Hafez. (2014). Design and Implementation of Video Conferencing Cloud-based Network using VoIP for Remote Health Monitoring in Telemedicine System. International Journal of Computer Informatics & Technological Engineering IJCITE, INDIA. 1.

[3] Frost, Aidan and Sullivan,(2006). Delivering on the Promise of Easy to Use, Secure, and Inexpensive Video Conferencing in and IP Environment. Palo Alto, CA 94303-3331, USA.

[4] Gal, O. (2020, April 1). The Facts Around Zoom and Encryption for Meetings/Webinars. Zoom.us. Retrieved from https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

[5] Hodge, R. (2020, May 8). Zoom security issues: Zoom buys security company, aims for end-to-end encryption. CNET. Retrieved from https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption/

[6] ITU-T (2003). Security in Telecommunications and Information Technology. International Telecommunication Union.

[7] Lazar, I. (2019, July 12). The Rise of Cloud Video Conferencing in Financial Services. Zoom.us. Retrieved from https://blog.zoom.us/wordpress/2019/07/12/rise-of-cloud-video-conferencing-in-financial-services/

[8] O'Flaherty, K. (2020, April 4). https://www.forbes.com/sites/kateoflahertyuk/2020/04/04/new-zoom-user-blow-this-is-how-thousands-of-video-chats-are-available-for-anyone-to-view-online/#37d6686e785d. Forbes. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2020/04/04/new-zoom-user-blow-this-is-how-thousands-of-video-chats-are-available-for-anyone-to-view-online/#2d85f789785d

[9] Peter Honeyman et.al (1998). Secure Videoconferencing. USENIX Security Sysposium, San Antonio, texas.

[10] Rop, K.V. & Bett, Nelson. (2012). IP BASED SECURITY ON VIDEO CONFERENCING.

[11] Statt, N. (2020, April 5). Google bans its employees from using Zoom over security concerns. The Verge. Retrieved from https://www.theverge.com/2020/4/8/21213978/google-zoom-ban-security-risks-hangouts-meet

[12] Tim Chown and Ben Juby (2004). Security Guide for H.323 Videoconferencing. The JNT Association, No. GD/VTA/009.

[13] Wakefield, J., 2020. Zoom boss apologises for security issues and promises fixes. BBC, [online] Available at: <https://www.bbc.com/news/technology-52133349> [Accessed 15 May 2020].

[14] Whittaker, Z. (2020, April 5). https://techcrunch.com/2020/04/05/zoom-new-york-city-schools/. Tech Crunch. Retrieved from https://techcrunch.com/2020/04/05/zoom-new-york-city-schools/

(This work is licensed under a Creative Commons Attribution 4.0 International License.)