International Journal of Computer Applications (0975 - 8887)
Volume 183 - No.38, November 2021

A Hybrid of two Homomorphic Encryption Schemes for Cloud Enterprise Resource Planning (ERP) Data

Arnold Mashud Abukari
Faculty of Applied Science and Technology
Tamale Technical University
Tamale, Ghana

Edem Kwedzo Bankas
School of Computing and Information Sciences
C.K. Tedam University of Technology and Applied Sciences
Navrongo, Ghana

Mohammed Muniru Iddrisu
School of Mathematical Sciences
C.K. Tedam University of Technology and Applied Sciences
Navrongo, Ghana

ABSTRACT

Data confidentiality and privacy has been one of the major challenges in cloud Enterprise Resource Planning (ERP) deployment. There are different techniques to help provide enhanced security and data confidentiality. In this paper, a hybrid of two different Homomorphic encryption schemes is proposed to further enhance security and data confidentiality of ERP data. The Paillier and RSA Cryptosystems are modified and applied to form a two-layer encryption scheme. A successful implementation of the proposed hybrid of two homomorphic encryption scheme without sharing keys with the cloud is realised. The security of the Cloud ERP Data is enhanced by the modification of the Paillier Cryptosystem with the introduction of a new parameter g_f to the Paillier Cryptosystem. The scheme also introduced a random parameter r_g to help generate the value of g_f. The simulation results reveals that the proposed scheme achieved improvement in the encryption time, decryption time and better throughput when compared with other schemes. The proposed scheme achieved six (6) percent improvement on encryption time,about thirty-two (32) percent improvement in decryption time as well as seven (7) percent improvement on throughput.

General Terms

Homomorphic Encryption, Cloud ERP Data

Keywords

Proxy Re-encryption, Double-layer Encryption, Cloud, ERP, Cloud Computing, Paillier Cryptosystem, RSA Cryptosystem, Cryptosystem

1. INTRODUCTION

The use of Information Technology has contributed significantly in the industrial development of many businesses, institutions and individuals across the globe. The development has increased the total amount of data over the past years by nine times as reported in [1]. The report by [1] suggested an increase of double of the number every two years. Despite this increase in data globally, data processing, data security and data input still are problematic. [2] proposed a hybrid of two encryption schemes to address security challenges of Zoom conferencing system.

Encryption Schemes have been used in an attempt to secure data via the internet or in the cloud. A single-layer encryption approach was used which are still not guaranteed and are prone to Chosen Cyphertext Attacks. Since the single- layer encryption schemes are prone to Chosen Cyphertext Attacks (CCA),a double-layer encryption schemes were proposed. The existing double-layer encryption schemes allows the Cloud to serve as a Proxy in the encryption process. This approach still gives the cloud some level of control and ownership of a section of the encryption process. Simply put, the success of the existing double-layer encryption schemes depends on the Cloud service provider serving as a Proxy. There is therefore a problem allowing the Cloud to serve as a proxy. In this paper,a hybrid of two different Homomorphic Encryption Schemes is developed to secure Cloud ERP Data.

2. PROXY RE-ENCRYPTION

[3] was the first to work on re-encryption using the ElGamal cryptosystem.
According to [3], the sharing of outsourced data between users who have encrypted their data with public keys using an asymmetric cryptosystem is called Proxy Re-Encryption (PRE). The encrypted data is outsourced to a third party called Proxy which is the cloud.

The main objective according to [3] is to allow the proxy (cloud) to re-encrypt the ciphertext of the data from one user that can be decrypted with a private key of another user. This means, the user sending the encrypted data for re-encryption must provide a private key to the proxy. This scenario works well with a trusted

cloud service provider. The cloud service provider still owns a section of the encryption process and that is still problematic.

3. HOMOMORPHIC PROXY RE-ENCRYPTION

A Homomorphic Proxy Re-Encryption is a Proxy Re-Encryption which allows computational operations on the cyphertext without revealing the content in the cyphertext. A third party or the cloud serves as the proxy.

In [3],the first Homomorphic Proxy Re-Encryption was proposed based on ELGamal Cryptosystem. It was based on secret pieces of information called Secret Re-Encryption Key.

However, in 2006, [4] argues that the proposed scheme by [3] was bidirectional. [4] argues that [3] allows the proxy (cloud) to convert all ciphertext from one user to another user's public key. Hence making the public key for re-encryption to be that of the user receiving the data. [4] proposed a unidirectional Proxy Re-Encryption approach.

In the year 2007, an Identity-Based Proxy Re-Encryption was proposed by [5]. They merged PRE and Identity-based crytography (IBC). In IBC, one of the public keys of one of the users is derived from his/her identity like email address and PRE.

The Unidirectional approach proposed by [4] was achieved since the re-encryption key is dependent on the identity of the user. This allows the sender of the data to still have access after the re-encryption of the data.

Despite this remarkable achievement by [5] of obtaining a unidirectional approach to Proxy Re-Encryption (PRE) using ElGamel, [6] observed that the ElGamel scheme was expensive in terms of computational complexity compared to modular multiplication since they are based on bilinear pairing.

Considering the argument raised by [6], [7] proposed an asymmetric cross-cryptosystem re-encryption scheme instead of the bilinear pairing as seen in ElGamel related schemes. Their approach do not allow one user to share data with another. They do not process encrypted data by the cloud or proxy through Homomorphic Cryptosystems.

In 2017, [8] built on the concept of Homomorphism and proposed a homomorphic proxy re-encryption scheme which does not require a user to re-upload the data shared by another user. Their scheme was based on Paillier Cryptosystem with the help of a Secure Linear Congruential Generator (SLCG). All the computations are performed by the cloud(proxy).

4. PAILLIER CRYPTOSYSTEM WITH SECURE LINEAR CONGRENTIAL GENERATOR (SLCG)

[8] proposed a new way to compute the differences between encrypted data by Paillier before sending to a Secure Linear Congruential Generator (SLCG) which is also implemented in the Paillier cryptosystem environment.

applied the SLCG to generate encrypted pseudo random sequence of integers.

4.1 Paillier Cryptosystem

According to [9], the paillier cryptosystem is an asymemetric cryptosystem with partial homomorphic encryption properties.

Considering $((g,P_k),P_s)$ as the public and private keys of the Paillier Cryptosystem such that:

$$P_k = pq, \tag{1}$$

where p and q are two large prime integers. The P_s is also determined as:

$$P_s = (p-1)(q-1), \tag{2}$$

where Z_{P_k} = (0,1,2,3,...,P_k-1) and $Z^*_{P_k}$ denotes the integers that have multiplicative inverses modulo P_k.
g is selected $g \in Z^*_{P_k^2}$ such that:

$$g^{P_s-1} mod {P_k}^2 P_k \in Z^*_{P_k} \tag{3}$$

The encryption of $m \in Z^*_{P_k}$ using the Paillier Cryptosystem to generate a ciphertext of $c \in {Z^*_{Pk}}^2$ is given by:

$$c = Enc[m,r] = g^m r^{P_k} mod {P_k}^2, \tag{4}$$

where r is a random integer associated to m.

used this property to calculate the difference between Paillier Encrypted data.
The decryption of the ciphertext using the Secret Key P_s is:

$$m = Dec[P_s,P_k] = (c^{P_s}-1){P_s}^{-1} mod {P_k}^2 P_k mod P_k \tag{5}$$

Considering two or more plaintext m_1 and m_2, the Paillier cryptosystem allows linear addition and multiplication.

$$Enc[m_1,r_1] * Enc[m_2,r_2] = Enc[m_1+m_2, r_1 r_2] \tag{6}$$

In [8], the following equation was used to calculate the difference of the ciphers.

$$d = a - (b mod P_k) \tag{7}$$

where a and b are two integers with encrypted versions.

4.2 Secure Linear Congruential Generator(SLCG)

[8] proposed Homomorphic Proxy Re-encryption scheme that required the cloud to generate Paillier pseudo random sequence of integers. [8] proposed a Secure Linear Congruential Generator based on congruences and linear functions.

The SLCG is built based on [10] which is implemented into the Paillier encrypted domain to generate random sequence integers.

$$Enc[X_{n+1}, r_{n+1}] = Enc[X_n, r_n]^a Enc[c, r_c] = Enc[aX_n + c, {r^a}_n r_c] \tag{8}$$

4.3 Problems with Using SLCG with Paillier Cryptosystem

After studying the proposed solution by [8], The following were observed for studies:

(1) Encrypted data using Paillier cryptosystem are sent via the internet to the cloud. Since the encrypted data is sent via the internet to the cloud, it could be intercepted by an unauthorised user or hacker.

(2) Ciphertexts are encrypted using the same random value.
(3) The cloud is trusted to host the proxy re-encryption generator.
(4) Only Paillier cryptosystem is used in both environments.

5. HYBRID HOMOMORPHIC ENCRYPTION SCHEMES

As the concept of Homomorphic Encryption schemes seems to be gaining grounds as one of the breakthroughs in securing data in the cloud computing environment, many researchers are looking at still improving the concept to further enhance security in cloud especially for ERP Data and video conferencing applications hosted by the cloud.

in their paper captioned "Can Hybrid Homomorphic Encryption Schemes be Practical?" brought the attention of researchers to explore the possibility of enhancing cloud computing security through the application of a hybrid homomorphic encryption scheme.

In resisting against confidentially attacks, the hybridisation of schemes that are homomorphic seems to be the effective in overcoming limitations [11].

6. THE PROPOSED SCHEME

This research work is proposing a hybrid of two different Homomorphic Encryption Scheme for Cloud ERP data that addresses the problems identified in the [8] proposed system.

The possibility of encrypted data being intercepted by unauthorised users, the cyphertexts generated using the same random value, trusting the cloud to host the proxy re-encryption generator were some of the problems identified that needs to be addressed. [12] used only RSA to do the double-layer encryption.

This means a hacker who is an expert in RSA decryption process can intercept and decrypt the data possibly. The proposed system also does not allow the cloud to conduct Proxy Re-Encryption on the ERP Data. The proposed system also enhances the security of Cloud ERP Data in the event the encrypted data is intercepted by unauthorised users.
This paper used Paillier and RSA encryption schemes

6.1 First Layer Encryption Using Paillier Cryptosystem

The research used the fast Paillier Cryptosystem as the first layer encryption. The Key Generation, Encryption and Decryption algorithms used the proposed scheme by (Paillier, 1999). Considering $((g,P_k),(P_k))$ as the public and private keys respectively of the Paillier Cryptosystem such that:

$$P_k = pq \tag{9}$$

where p and q are two large prime integers.
The (P_k) is also determined as:

$$(P_k) = (p-1)(q-1) \tag{10}$$

g is selected $g \in Z^*_{P_k^2}$ such that:

$$g^{(P_k)-1} mod {P_k}^2 P_k \in Z^*_{P_k} \tag{11}$$

The encryption of $m \in Z^*_{P_k}$ using the Paillier Cryptosystem to generate a ciphertext of $c \in Z^*_{P_k^2}$ is given by:

$$c = Enc[m,r] = g^m r^{P_k} mod {P_k}^2, \tag{12}$$

where r is a random integer associated to m.

It is possible to generate a fast version of the equation 2.4 proposed by (Paillier, 1999) by letting $g_f = r_g + g$ without reducing security. This will reduce the encryption of m to c will require only one exponential and two modulo multiplications resulting in:

$$c = Enc[m,r] = (1 + mP_k) r^{P_k} mod {P_k}^2 \tag{13}$$

where r is a random integer associated to m. From (Paillier, 1999), we generated a better version of the equation 2.4 into equation 3.5 by letting

$$g_f = r_g + g \tag{14}$$

without reducing security.
This will reduce the encryption of m to c and will require only one exponential and two modulo multiplications resulting in:

$$c_1 = Enc[m,r] = (1 + mg_f) r^{g_f} mod {P_k}^2 \tag{15}$$

Decryption is not done at the first layer algorithm. The c_1 is passed to the second layer as a plaintext.

6.2 Second Layer Encryption

In the proposed scheme, the ciphertext of the first layer encryption algorithm c1 is treated as a plaintext and further encrypted using the RSA Cryptosystem.

$$P_k^* = P_k \tag{16}$$

$$P_s^* = (n) \tag{17}$$

where P_k^* and P_s^* are the public and secret keys respectively of the second layer encryption.
Select e such that:

$$GCD(e, P_s^*) = 1 \tag{18}$$

Determine the value of $(n)^*$ from:

$$(n)^* = 1 mod P_s^* e \tag{19}$$

The second layer set of public key generated are e and P_k^*. The secret(private) key is $(n)^*$. The second layer encryption is computed using:

$$c_2 = c_1^r . e mod P_k^* \tag{20}$$

where c_1 and c_2 are the ciphers from the first and second encryption respectively.

6.3 Decryption Phase

In the quest to decrypt the hybrid of two different encryption scheme, the research applied the RSA decryption algorithm to get c_1 followed by the paillier cryptosystem decryption algorithm to get back the cloud ERP Data as follows:

$$c_1 = c_2 * (n)^* mod P_k^* \tag{21}$$

$$m = L(c_1^{(P_k)} mod P_k^2) L(g_f^{(P_k)} mod P_k^2) mod P_k \tag{22}$$

where

$$L(x) = x - 1 P_k \tag{23}$$

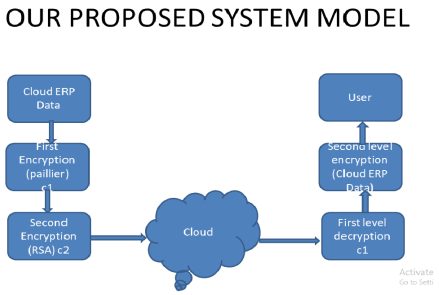

Fig. 1. Proposed System Model

6.4 Conditions for the Proposed System

In order for the proposed scheme to work effectively the following conditions needs to be satisfied:

1. Z_{P_k} = (0,1,2,3,...,P_{k-1})
2. $Z^*_{P_k}$ are integers with multiplicative inverses modulo P_k
3. $g \in Z^*_{P_k^2}$
4. g is selected from $Z^*_{P_{k-1}^2}$. This condition is necessary to limit the choice of the selection of g.
5. The order of g must be multiple of P_k and invertible
6. $g_f = r_g + g$
7. The value for g must satisfy the Carmichael's theorem that $g^{\lambda(P_k)} \equiv 1 mod P_k$
8. $m \in Z^*_{P_k}$
9) The value of r_g must be a non-negative number.
10) In situations where the value of r_g is non-zero, then the proposed value must be coprime to both p and q.

7. RESULTS AND DISCUSSIONS

The research work applied the Paillier cryptosystem and the RSA Algorithm to develop a hybrid of two different Homomorphic Encryption scheme to secure Cloud ERP data homomorphically.

In order to guarantee optimum strength in security with the proposed scheme, both the proposed first layer encryption and second layer encryption must have n (key size) values of 2048 bits long according to [13]. This means both encryption layers should have not less than twice the size due to the n_2 modulus in each encryption layer in their operations.

The Paillier and RSA algorithms keys are generated through a modulus P_k and P^*_k respectively and which is used to determine the strength of the encryption scheme.

According to [13], the recommended security strength begins with $n = 2048$ which according to them is estimated to support a security strength of 112 bits but a higher additional key length is supported.

The best known attacks on Paillier and RSA are chosen cipher Attacks(CCA) with number field sieving or prime factorisation. Against this background, the research proposed and successfully implemented a hybrid of two homomorphic encryption schemes without sharing keys with the cloud which houses the ERP Data.

A new parameter g_f is introduced into the Paillier Cryptosystem to increase the strength of the security since it will be relatively more time consuming to find the value of g_f compared to the value of g being used by Paillier Cryptosystem.

The introduction of g_f has helped to enhance the security of Cloud ERP Data. In the quest to generate the value of g_f, a random value r_g was used. The random parameter r_g is selected based on some proposed conditions. This helps to make the guessing of the proposed new parameter g_f very difficult and thereby increasing security for the Cloud ERP Data. The time needed to break our scheme will be $O(n_1 + n_2)$, where n_1 and n_2 are the security length of the first and second encryption respectively.
The proposed scheme can only be broken in the unlikely situation of:

$$e^{((1+o(1))(329log(n_1+n_2))^{1/3}(loglog(n_1+n_2))^{2/3})} \quad (24)$$

7.1 Evaluation Parameters

The quest to evaluate the performance of the proposed solution against those proposed by [8] and [12], the research work used the Encryption time taking the computational time and response time into consideration, the decryption time, the size of the encrypted file size, size of the decrypted file size and the throughput.

The simulation was done on a computer having intel(R) Core(TM) i5-3317U CPU@1.70GHz processor and 8GB RAM with a 64-bit Operating system. Python was used as the experiment compiler and simulator. The thesis used a 1024 and 160 bits for RSA and Paillier based encryption per the NIST recommendation (1024bits(RSA)=160bits(Paillier)). File size of 14MB and 7MB was used in the simulation.

7.2 Encryption Time Analysis

The research used a standard data transmission calculator to calculate the data transfer time that was added to the time of running the algorithms to determine the encryption time for the respective schemes.

A 14MB with a 128Mbs transfer rate will result in a transfer time of 0.834465 seconds in a very reliable internet connection and a 7MB will be transfered in 0.417233 seconds.

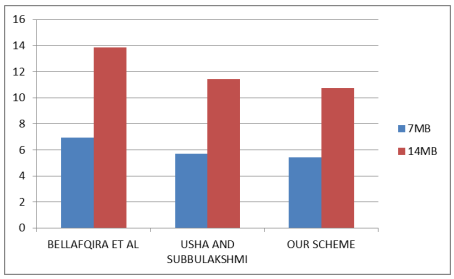

Fig. 2. Encryption Time Analysis

The experimental results shown in figure 2 shows the proposed scheme performs better than the existing schemes by [8] and [12] in a very stable and reliable internet. The figure 2 further shows that

the proposed scheme will even perform far better than the existing schemes compared with in an unreliable internet environment.

7.3 Decryption Time Analysis

The experimental results for decryption time of the proposed scheme compared to [8] and [12] is presented in figure 3.

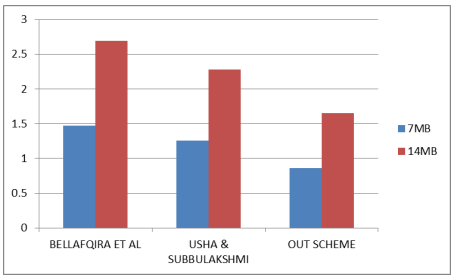

Fig. 3. Decryption Time Analysis

The experimental results on the decryption time suggests the proposed scheme uses less computational resources and response time. Just like the encryption time analysis, the other existing schemes may even perform further poorly in an unstable internet environment.

7.4 Throughput Analysis

Throughput is defined as the average rate of a successful delivery of data or message over a communication channel. The research analysed the plaintext in bytes encrypted by their respective time. This analysis is important since the higher the throughput, the higher the performance.

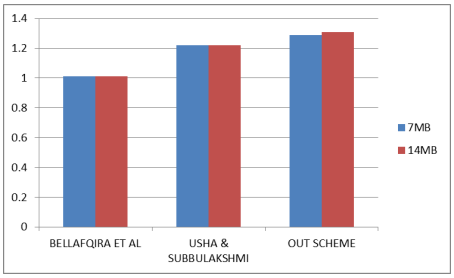

Fig. 4. Throughput Analysis

The output of the throughput analysis suggests the proposed scheme has a higher throughput compared to the schemes proposed by [8] and [12]. A higher throughput means a better performance as indicated in figure 4.

8. CONCLUSION

Implementation of the proposed scheme will guarantee data privacy and confidentiality in CCA(Chosen Ciphertext Attacks) by Unauthorised users or hackers.

The proposed Hybrid of two different Homomorphic encryption scheme has been demonstrated to perform better compared to other schemes. The proposed scheme, per the experimental results uses less computational resources and has faster response rate as well as has a higher throughput.

The proposed Hybrid of two different Homomorphic encryption scheme when implemented will enhance security and ERP Data privacy in cloud as well as help implement the solution architecture proposed by [2].

An implementation of the proposed scheme will secure video and audio data generated which can only be decrypted by the zoom user. In the event of a conference meeting, video and audio files are being intercepted by other third-party, the proposed scheme 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.

9. REFERENCES

[1] Gantz, J. and Reinsel, D. (2011). Extracting value from chaos. Framingham, MA: International Data Corporation. Retrievedfrom www.emc.com/collateral/analyst.../idc-extracting-value-from-chaos-ar.pdf (Archived by WebCite® athttp://www.webcitation.org/6bZoomByo)

[2] Abukari, A.M. and Bankas, E.K. and Iddrisu, M.M. (2020). A Secured Video Conferencing System Architecture using A Hybrid of Two Homomorphic Encryption Schemes: A Case of Zoom. International Journal of Engineering and Technical Research. 9. 237.

[3] Blaze,M., Bleumer,G. and Strauss,M. (1998). ?Divertible protocols and atomic proxy cryptography,? in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1998, pp. 127?144.

[4] Ateniese,G., Fu,K., Green,M., and Hohenberger,S. (2006). ?Improved proxy re-encryption schemes with applications to secure distributed storage,? ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1?30.

[5] Green, M. and Ateniese,G. (2007). ?Identity-based proxy re-encryption,? in Applied cryptography and network security. Springer, pp. 288?306.

[6] Baek, J., Safavi-Naini, R. and Susilo,W. (2005). ?Certificateless public key encryption without pairing,? in International Conference on Information Security. Springer, pp. 134?148.

[7] Deng,R. H., Weng,J, Liu,S., and Chen,K. (2008). ?Chosen-ciphertext secure proxy re-encryption without pairings,? in International Conference on Cryptology and Network Security. Springer, pp. 1?17.

[8] Bellafqira,R., Coatrieux,G., Bouslimi,D., Gw enol e Quellec and Cozic, M. (2017). Sharing Data Homomorphically Encrypted with Different Encryption Keys.arXiv:1706.01756v1 [cs.CR].

[9] Paillier, Pascal (1999). "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". EUROCRYPT. Springer. pp. 223–238. doi:10.1007/3-540-48910-X-16.

[11] Khalid El, M., Abdellah, E. and Abderrahim, B.H.(2015). "Challenges of using homomorphic encryption to secure cloud computing", in International Conference on Cloud Technologies and Applications(CloudTech), Marrakech, Morocco.

[12] Usha, D. and Subbulakshmi,M. (2018). Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud. International Journal of Scientific and Engineering Research, 9(5). Retrieved july 2019

[13] Barker, E. and Roginsky, A. (2019), Transitioning the Use of Cryptographic Algorithms and Key Lengths, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-131Ar2 (Accessed November 18, 2021)

[14] Bill, M and 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/.

[15] Cezar, P., Mihai, T. and Cristian, L. (2016). "Homomorphic Encryption Based on Group Algebras and Goldwasser-Micali Scheme" in Innovative Security Solutions for Information Technology and Communications, Bucharest, Romania, pp. 149-166.

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

[17] Frost, A. 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.

[18] Gal, O. (2020). 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/.

[19] Grabot, B., Mayere, A. and Bazet, I.(2008). ERP Systems and Organisational Change, London: Springer London. Available at: http://www.springerlink.com/index/10.1007/978-1-84800-183-1[Accessed September 1, 2017]

[20] Guo, S., Xu, H.: (2015) A secure delegation scheme of large polynomial computation in multi-party cloud. International Journal of Grid and Utility Computing, 6(2), pp.1-7.

[21] Han,J.,Susilo,W. and Mu,Y. (2013). ?Identity-based data storage in cloud computing,? Future Generation Computer Systems, vol. 29, no. 3, pp. 673?681.

[22] Hodge, R. (2020). 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/.

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

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

[25] Lazar, I. (2019). 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/

[26] Liang,X., Lu,R., Lin,X. and Shen,X. S. (2010). ?Ciphertext policy attribute based encryption with efficient revocation?, Technical Report, University of Waterloo.

[27] Liang,X., Cao,Z., Lin,H., and Shao,J. (2009). ?Attribute based proxy re-encryption with delegating capabilities,? in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, pp. 276?286.

[28] Marklow, A. and Todd, F.(2014). "A first Course in Abstract Algebra: Rings, Groups, and Fields", 3rd edn. CRC Press, Taylor and francis Group.

[29] Rabah, K. (2006). Implementing Secure RSA Cryptosystem Using Your Own Cryptographic JCE Provider. Journal of Applied sciences, 6(3); 482-510.

[30] Rop, K.V. and Bett, N. (2012). IP BASED SECURITY ON VIDEO CONFERENCING.

[31] Singh, S., Preet and Maini, Raman. (2011). ?Comparison of Data Encryption Algorithms?, International Journal of Computer Science and Communication, vol. 2, No. 1, pp. 125-127.

[32] 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

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

[34] 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].

[35] Whittaker, Z. (2020). 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/

[36] Xu,P., Jiao,T., Wu,Q., Wang,W. and Jin,H. (2016). ?Conditional identity-based broadcast proxy re-encryption and its

application to cloud email,? IEEE Transactions on Computers, vol.
65, no. 1, pp. 66?79.