KawalPilpres2019: a highly secured real count voting escort architecture

Onno W. Purbo*[1], Gildas Deograt[2], Rolof Satriyanto[3], Abraham Ferdinand[4], Pamadi Gesang[5], Rendra Kesuma[6], Kalpin Erlangga Silaen[7]
[1,2,3,4,5,6,7]XecureIT.id, 2 Raya Jatiwaringin St., Cipinang Melayu, Jakarta, Indonesia
[1]IBI Darmajaya (Graduate Study, Computer Science, IBI Darmajaya),
93, A. Z. Pagar Alam St., Labuhan Batu, Bandar Lampung, Indonesia
*Corresponding author, e-mail: onno@indo.net.id[1], gildas.deograt@xecureit.id[2],
rolof.satriyanto@xecureit.id[3], abraham.ferdinand@tnisiber.id[4], pamadi.gesang@tnisiber.id[5],
rendra.kesuma@tnisiber.id[6], kalpin.silaen@xecureit.id[7]

Abstract

This paper reports on the highly secured information security architecture used by the KawalPilpres 2019 to escort Voting Commission (KPU) data entry. For the first time, a voting escort implements ISO 27001 compliance information security. As of 15 May 2019, 9550 volunteers reported 482,602 voting data of 336,445 voting booths, both in the country and overseas, through the micro-apps KawalPilpres2019. PeSanKita is used as a secure communication channel and to run micro-apps KawalPilpres2019. Double Ratchet Algorithm secures the channel. Different from other voting escort initiatives, KawalPilpres2019 uses (1) primarily C1 Plano photo, (2) no upload limit per voting booth, (3) no web upload, rather via PeSanKita Secured Platform. Behind the scenes, the verification process is done twice before displaying data to the publicly accessible monitoring web. The result is a robust voting escort system, difficult to hack and guarantee data integrity. Guaranteed security, availability, and data integrity are the main requirements for future eVoting systems.

Keywords: *eVoting, highly secured information infrastructure, KawalPilpres, PeSanKita, voting escort*

1. Introduction

General Election is the key to the gate of democracy of a nation that must be guarded every five years. The existence of the Voting Commission (KPU) assisted by Voting Monitoring Body (BAWASLU), which was supported by many electoral data escort communities, became very important. The 2019 Indonesian presidential election was an important milestone, where the number of voting escort guarding the result was increased significantly as compared to the 2014 Indonesian presidential election. The escort initiatives perform real vote counting, not a sampling quick count approach [1, 2]. The technology used by these data voting escorts is very diverse, but in general has the same characteristics, namely, (1) use the web as a means for data transactions/shipments, (2) web to upload, and view the data on the same web channel, and (3) some receive aggregate data at the district or sub-district level to speed up the calculation processes [1].

KawalPilpres2019 was one of the data voting escort initiative. KawalPilpres2019 was part of the Gerakan Ayo Nyoblos Ayo Pantau, a civil society movement echoed by various institutions and communities to encourage the active participation of the people in helping to bring about Peaceful and Quality Elections. In addition to inviting the public to exercise their right to vote, this movement also invites the public to monitor the election process and report on the results of the presidential election. This movement is open to all elements of society to love the Republic of Indonesia and want a better democratic process in Indonesia [3].

In this work, the C1 Plano photo would be the critical reference data. C1 Plano is a large poster posted in front of Voting Booth and used to manually calculate the voting result of a particular voting booth [4, 5]. Since it is posted in front of the voting booth and, thus, anyone may take a photo of the C1 Plano as evidence. The ability for all to take the C1 Plano photo is an important security feature and heavily exploited in this work.

Received May 29, 2019; Revised July 2, 2019; Accepted July 18, 2019

2. Design of KawalKita2019 in a Highly Secured Information Security Architecture

2.1. Secure Network Architecture

For simple data entry, the scenario can be straightforward. A data entry officer can enter a voting data summary from the voting booth (TPS) into the database and then display the results to the Web. For a simple scenario, the system architecture does not need to be complicated. It can be made very simple so that all processes can run quickly. For example, it requires only (1) data entry components, (2) database component, and (3) web components.

Since security, accuracy, availability, and data integrity are a top priority, the system architecture must be dramatically changed. In the case of national presidential voting, security, accuracy, availability, and data integrity is a high priority. A Highly Secured Information Infrastructure must be adopted and used in the system [6, 7]. In this work, lead by Gildas Deograt, the team design and implement a highly secured information infrastructure to meet the stringent security requirements. Many of the technical development team member are a certified ISO 27001 auditor, such as CISSP, CISA, CEH certified. For the first time, a voting escort implements ISO 27001 compliance information security.

Some of the security features that are visible and different from other initiatives are the primary data used is C1 Plano directly from the voting booth, which can be obtained through photos by everyone. The number of uploads per voting booth is not limited and can be simultaneously performed from many smartphones/sources. Voting data entry does not use the Web at all, instead of an entirely different communication channel on the PeSanKita Secured Platform. Finally, behind the scenes, the verification process is done twice before displaying data of the voting booth to the Web and, thus, everyone may monitor the calculation results. The result is a robust voting escort system, difficult to hack and at the same time guarantee the integrity of the data displayed so that it is always confirmed with field data. Guaranteed security, availability, and data integrity are the main requirements if a system is used in a future eVoting system.

2.2. Possible Errors and Attacks on the System

Errors and attacks can occur in many places, at various levels, such as at a voting booth at the time of data entry. Some errors may be incorrect writing of data, not suitable C1 Plano Photos, such as out of focus, blurred. C1 Plano photo was taken when the data is incomplete, such as lack of officer signature, voting booth info, district info. Other errors raised when there was a change in the number of voting booths cause by sudden additional voting booths. Besides, an attacker to the system may intentionally submit the wrong C1 Plano photo.

At a higher level, such as sub-district, district, province, during voting accumulation process, some errors/attacked may be incorrect writing of data. An attacker may intentionally damage the C1 Plano poster. Besides, an attacker may hack the network and communication channels [8, 9]. At the national level, some of the errors may be incorrect data entry. An attacker may make more elaborate attacks, such as an attack on communication channels [8, 9], such as a MiTM (Man in the Middle) attack [10, 11]. Attacks on the monitoring web, such as command injection [12], Distributed Denial of Service (DDoS) [13, 14], Cross Site Scripting (XSS) [15, 16]. Attacks on databases, such as SQL Injection [17, 18].

Highly Secured Voting Escort Architecture Figure 1 shows the global picture of highly secured voting escort architecture used in KawalPilpres2019. While the backend architecture is more complicated as compared to the front end with a relatively simple user interface and processes. The front end section is basically,

- Pantau Web Page-containing a summary of the accumulated voting result. From the web interface, one may drill down the data into a particular voting booth and obtain various data including the C1 Plano picture, voting booth information as well as the number of votes.
- KawalPilpres2019 micro-application-allowing anyone who installs the application to participate in uploading the Voting data. One may upload many unlimited voting booth data. The KawalPilpres2019 micro apps reside in the PeSanKita Secured Platform.

There are several end-to-end secured chat approaches [19-24]. Whatsapp seems to have the largest user-based among end-to-end secured chat [24]. To meet the end-user comfortably level, the user interfaces design of PeSanKita Secured Platform similar to Whatsapp. Thus, for a common user, PeSanKita is relatively similar to the instant messaging or chat platform, especially Whatsapp. In this work, a PeSanKita Secured Platform has been extended not only to accommodate chat but also to run micro-applications [25, 26].

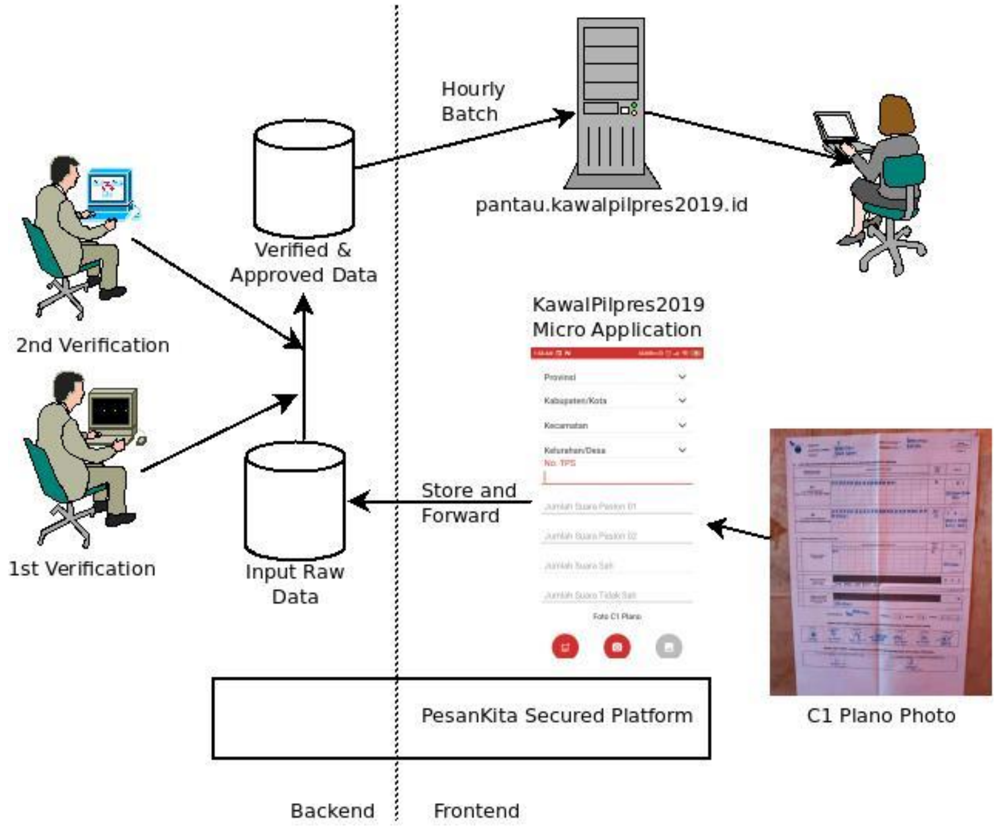


Figure 1. Overview of KawalPilpres2019

From the user point of view, a quite complex installation process, including a secure authentication process is apparent. PeSanKita uses SMS to authenticate a particular smartphone. Upon completion of the authentication process, the key pair is generated to secure the communication platform. The generated key is part of the Double Ratchet Algorithm (previously referred to as the Axolotl Ratchet [27]) similar to Whatsapp [28, 29].

Trevor Perrin and Moxie Marlinspike in 2013 developed the Key Management Algorithm [29]. The algorithm can be used as part of a cryptographic protocol for end-to-end encryption in instant messaging. After the initial key exchange, the algorithm manages short-lived session key updates and maintenance. This technique combines cryptographic ratchet based on the Diffie-Hellman key exchange (DH) and ratchets based on the Key Derivation Function (KDF) such as, for example, hash functions and is therefore called double ratchet. The algorithm can self-healing that later known as Future Secrecy, or Post-Compromise Security. The backend process is much more complicated. The voting data submitted by KawalPilpres2019 volunteers is stored in a database. The database engine equipped with High Availability (HA) to ensure data availability and integrity.

Any uploaded voting data is not directly visible in publicly available pantau.kawalpilpres2019.id web page. To ensure the uploaded information is secured, the KawalPilpres2019 system carries out security testing to ensure the integrity of uploaded voting data is guaranteed. This process, in turn, removes any gap that enables other parties to change the uploaded voting data illegally. The verification tests are carried out by an independent team, which is a team outside the development team. Since the verification test carried out by a separate team, the tendentious nature is not present.

A rigorous verification process is carried out on a separate web application from the data entry system. Verification is carried out by trusted volunteers, called moderators. To be a moderator, users must get approval from a promoter and must complete data such as citizen ID and email address. The verification mechanism starts by providing random polling data for verification. The moderator can see the C1 Plano report from the voting booth. Since the submitted voting data can be more than one, the moderator may review and select the valid voting data. At least two moderators have to verify a particular submitted voting booth data to This approach is an implementation of dual control to minimize human error or fraud in the verification process.

After at least two moderators validate the particular voting booth data, the system journalizes the voting booth data into tabulation data and ready to be displayed on the Pantau web server. The voting booth data that has been journal-ed does not go directly to the web server. The backend database server will hourly batch the tabulated voting data into the Pantau web server. The pantau.kawalpilpres2019.id web server is a static application with no database connection. Thus, there is virtually no security hole on the web server that can be used by an attacker to exploit the KawalPilpres2019 database. Automatic hourly batch processing was carried out to ensure that data on Pantau web is always updated. Besides, a manual batch process is still available if needed at any time.

3. Implementation of KawalKita2019

The activation of KawalPilpres2019 requires an additional authentication process. The authentication requires the use of a real name as written in the identity card. The authentication subject is the user, not the application, and, thus, only registered users can enter C1 Plano data entry at the voting booth (TPS) level. Authentication techniques use basic authentication with credentials in the form of randomly generated passwords (a combination of numbers and letters) to ensure a 'strong' password so that it is not easily broken into by a brute force attack. The whole installation and approval of KawalPilpres2019 take approximately 5-10 minutes depending on the speed of the Internet.

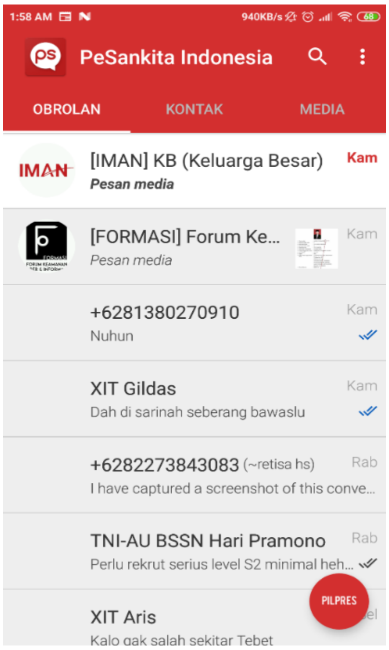
Since the system relies heavily on the authenticity of the voting booth data captured on C1 Plano, defense techniques against fake C1 Plano are essential. The system allows many submissions of C1 Plano for a particular voting booth to layered the defense. It is to say; one smartphone may enter data for many voting booths. However, one smartphone can only enter data for a particular voting booth once. With this technique, the moderator has much information to analyze fake C1 Plano data. In the end, fake data can be minimized.

In submitting the voting booth data, the micro-application KawalPilpres2019 uses HTTPS with an SSL certificate belonging to the backend service validated by micro apps to establish secure communication with the backend service. The actual communication process is connectionless, store and forward, process. Thus, KawalPilpres2019 requires minimal server resources even for handling many upload data connections. Shown in Figure 2 is the typical PeSanKita interface viewed by most users. It is relatively similar to Whatsapp and used mainly for chatting and group discussion. At the bottom right, the users may see a red dot "PILPRES", and it is the micro-application KawalPilpres2019 used to submit voting data into KawalPilpres2019 system. Most people may become volunteers in voting data submission via PeSanKita Secured Platform as PeSanKita is freely available both the Android Play store as well as the iPhone.

Shown in Figure 3 is the main menu of the Kawal Pilpres2019 micro-application. The primary menu is the six dots at the bottom of the main menu. To see the summary of verified voting data accumulated at Kawal Pilpres2019, one can click the “PANTAU” menu which then redirects to Pantau Web page over the Internet. One may also invite friends to participate as a volunteer in gathering and uploading voting data in KawalPilpres2019 by clicking the "UNDANG TEMAN” menu. For voting booth data submission, one can click the "LAPOR" menu. To view the one's submitted data, one may click the "LAPORAN" menu.

Figure 4 shows the menu after one click the "LAPOR" menu. The design of the voting data submission menu is simple enough to minimize any error done by the volunteers. First, one should upload the correct C1 Plano picture from either the smartphone gallery or take the picture directly. Most of the time, one will likely to submit the C1 Plano picture from the smartphone gallery. One may then enter the voting booth number at any time. The KawalPilpres2019 knows the maximum number of a voting booth at a particular location/village and is used as the maximum limit of voting booth number. The location information is pre-programmed via scroll down list. First, one has to select the province, then select the districts, then select the sub-district, and finally, the actual location or village. Thus, there is a small possibility for error in voting booth location as all information is pre-programmed as selectable list data.

One may enter the voting data into the system after completed the voting the information. One submits the voting data for first candidate, second candidate as well as abstain. However, as a protection feature, the sum of a first and second candidate, i.e., the total legitimate voters, is calculated by the application, and is used for cross check with the uploaded C1 Plano picture. Thus, there is a small possibility for error in the sum of legitimate voters.



[IMAN] KB (Keluarga Besar) Kam
Pesan media

[FORMASI] Forum Ke... Kam
Pesan media

+6281380270910 Kam
Nuhun

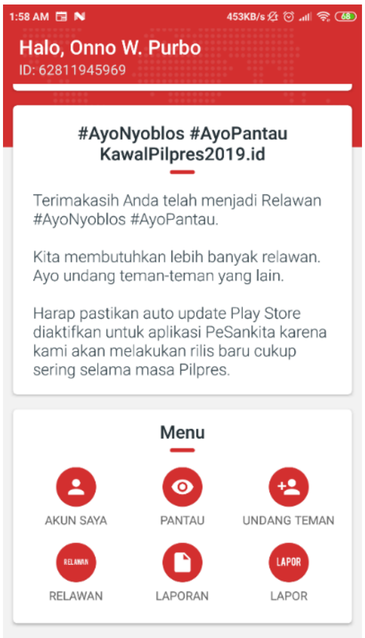
XIT Gildas Kam
Dah di sarinah seberang bawaslu

+6282273843083 (~retisa hs) Rab
I have captured a screenshot of this conve...

TNI-AU BSSN Hari Pramono Rab
Perlu rekrut serius level S2 minimal heh...

XIT Aris
Kalo gak salah sekitar Tebet

Figure 2. PeSaKita Interface



Halo, Onno W. Purbo
ID: 62811945969

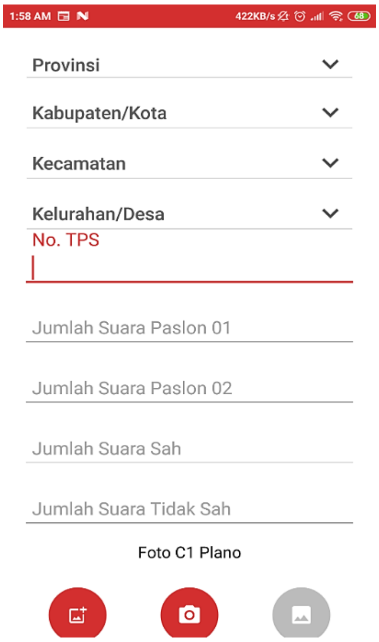
#AyoNyoblos #AyoPantau
KawalPilpres2019.id

Terimakasih Anda telah menjadi Relawan #AyoNyoblos #AyoPantau.

Kita membutuhkan lebih banyak relawan. Ayo undang teman-teman yang lain.

Harap pastikan auto update Play Store diaktifkan untuk aplikasi PeSankita karena kami akan melakukan rilis baru cukup sering selama masa Pilpres.

Figure 3. KawalPilpres2019 Main Menu



Provinsi

Kabupaten/Kota

Kecamatan

Kelurahan/Desa

No. TPS

Jumlah Suara Paslon 01

Jumlah Suara Paslon 02

Jumlah Suara Sah

Jumlah Suara Tidak Sah

Foto C1 Plano

Figure 4. KawalPilpres2019

3.1. Communication Flow During Voting Escort

As shown in Figure 5, A complex system involving lots of volunteers rely heavily on the communication flow among each party. Seamless communication between the various stakeholders strengthens the public's trust towards the KawalPilpres2019. Communication media used are both one and two-way media. The one-way information delivery is via the Pantau web at https://pantau.kawalpilpres2019.id/ - to provide voting data for the public via the Internet. Two ways communication media via (1) Twitter @kawalpilpres, (2) PeSanKita +6217042019, and (3) Whatsapps +62818250475. Two-way communication is vital. Most people and communities want to get answers on many aspects of KawalPilpres2019 as well as other voting-related issues. Rapid answer via social media as well Whatsapp creates a comfortable environment and, thus, increases trust. Twitter is very instrumental in spreading general information to many people at once as well as holding a large scale group interaction. Twitter interaction can even match the group communication platform in interaction. All ultimately increases public trust towards KawalPilpres1919. An increase in the trust is apparent in a large number of volunteers, exceeding 9500 volunteers, who participate in KawalPilpres2019.

In the process, at first, many people on the Internet are monitoring the web https://pantau.kawalpilpres2019.id/ and generally compared to other voting escort initiatives as well as the national voting commission (KPU) data on the web. People typically start questioning the lack of data of their voting booth on Pantau web via Twitter, and Whatsapp. In response, Kawalpilpres volunteers may request the C1 Plano data if any as well as provide suggestions to upload C1 Plano voting data to the KawalPilpres2019 via PeSanKita available free from play store. If there is any error visible on the Pantau web, people typically mention via Twitter/Whatsapp. This message then passes to the moderators in the backend of the KawalPilpres2019 system to correct the information. The whole communication process, in turn, creates a solid foundation for trust in KawalPilpres2019.

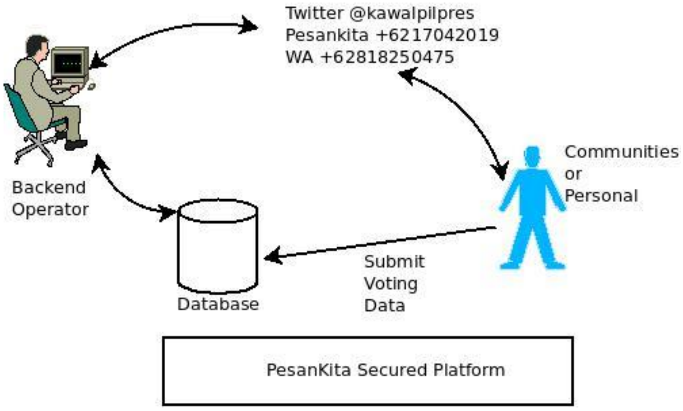


Figure 5. Communication flow in KawalPilpres2019

4. Results and Difficulties on the Ground

As of Wednesday 15 May 2019 00:00, a total of 9550 volunteers reported 482,602 data (C1 Plano vote picture or copy of the 2019 presidential election) of 336,445 voting booths (41.52% of total voting booths) in the country as well as overseas, through the micro-application KawalPilpres2019 in the PeSanKita application. With approximately 60 active moderators, KawalPilpres2019 ables to verified 89,646 of voting booth (TPS) data, 11.06% of the total national voting booths. These data are accessible through the Pantau web page. Some of the valuable lessons are (1) people need to be educated/socialized about the importance of the C1 Plano documentation especially for monitoring and escort process, and (2) the difficulty in verifying large amounts of voting data.

A standard on how to document to take the C1 Plano picture needs to disseminate. KawalPilpres volunteers found many incomplete photos of the C1 Plano form, such as no sign of the voting booth officer, picture from the wrong angle and make a truncated photo, unclear/blurred photos, or incomplete/incorrect voting booth (TPS) data. Verifying voting data is a time-consuming task, the 60 moderators with working hours of 12 hours per day are only able to check 3000 voting booth data/day or around four voting booth/hour/moderator. It is a lengthy process. As a result, within one month, the system was only able to verify 11.06% of the total voting booth (89,646 voting booth) to be included into the Pantau Web page for monitoring data of KawalPilpres2019.

5. Results and Difficulties on the Ground

In summary, trust is critical in any election process. Thus, it is crucial to secure the voting process during the election counting process. Micro-application KawalPilpres2019 demonstrates a secured and robust voting escort system for securing the voting counting process. The use of high-level information security architecture in the PeSanKita Secured Platform opens the possibility to implement such a robust voting escort system. Exceptional and responsive two-way communication via various channels helps increase the people's trust towards KawalPilpres2019 systems. Trust is the critical key for a success voting escort systems.

The authors want to suggest the election committee (KPU) and the election supervisor (BAWASLU) put extra effort in securing the input data, namely, C1 Plano. C1 Plano plays a vital role during the electronics vote counting process. The voting booth (KPPS) supervisors should participate in documenting/taking photos of the C1 Plano Form of the voting results on the voting day. Also, the authors strongly suggest using the electronic calculation system for highly secured information infrastructure for the efficiency and effectiveness of the whole voting system. Having an electronic voting calculation system in a highly secured information infrastructure, the voting commission may then perform an efficient upcoming voting process for more than 300 municipal and governor elections, as well as other government-people electronics interactions.

Acknowledgment

We want to thank all who have entrusted the voting calculations to KawalPilpres1919. Especially for all volunteers who helped upload C1 Plano data. Also, KawalPilpres2019 moderators who silently work in the backend. Moreover, various communities who help collect voting data, such as Beneran Indonesia, Forum Keamanan Siber dan Informasi (Formasi), Forum Nasional Perempuan Bhineka Tunggal Ika, Gema Mathla'ul Anwar, Gerakan Angkatan Muda Kristen Indonesia (GAMKI), Gerakan Damai Nusantara, Gerakan Indonesia Kita (GITA), Gerakan Kebangsaan Indonesia (GKI), Gerakan Mahasiswa Kristen Indonesia (GMKI), Gerakan Pemuda Ansor, Ikatan Mahasiswa Muhammadiyah, Indonesian Conference on Religion and Peace (ICRP), Jaringan Pendidikan Pemilih untuk Rakyat (JPRR), Jaringan Solidaritas NKRI, Komisi Kerasulan Awam KWI, Komite Pemilih Indonesia (Tepi), Komunitas Indonesia Hari Ini, Majelis Tinggi Agama Khonghucu Indonesia (MATAKIN), National Character Building Indonesia (NCBI), PARA Syndicate, Pena HAM, Perhimpunan Indonesia Tionghoa (INTI), Perhimpunan Mahasiswa Katolik Republik Indonesia (PMKRI), Persekutuan Gereja-Gereja di Indonesia (PGI), Pimpinan Pusat Pemuda Muhammadiyah, Sahabat Ansor, TPS & A5 Crisis Center.

References

[1] Budiarti E. Effectiveness of Election Guard as a New Alternative to Democratic Mechanisms (in Indonesia: Efektivitas Kawal Pemilu sebagai Alternatif Baru Mekanisme Demokrasi). Doctoral dissertation. Yogyakarta: Universitas Gadjah Mada. 2017.

[2] Setiawan A. The Role of Volunteers in Winning the Joko Widodo-Jusuf Kalla Couple in the 2014 PILPRES (in Indonesia: Peran Relawan dalam Pemenangan Pasangan Joko Widodo-Jusuf Kalla dalam PILPRES 2014). *KAIS (KAJIAN: Jurnal Ilmu-Ilmu Sosial)*. 2018; 28(1).

[3] Lestari Y. Civic Engagement Using Online Media Among Young People of Padang City (in Indonesia: Civic Engagement Menggunakan Media Online di Kalangan Anak Muda Kota Padang). *Jurnal Ilmu Komunikasi Efek.* 2017; 1(1).

[4] Purwanto A, Zuiderwijk A, Janssen M. *Citizen engagement in an open election data initiative: a case study of Indonesian's Kawal Pemilu.* Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. ACM. 2018; 62.

[5] Susanto A, Asy'ari H, Hardjanto US. Analysis of the Implementation of Duties and Powers of Election Supervisory Committees in Democratic General Election of President and Vice President in Semarang City in 2014 (in Indonesia: Analisis Pelaksanaan Tugas dan Wewenang Panitia Pengawas Pemilu dalam Pemilihan Umum Presiden dan Wakil Presiden yang Demokratis di Kota Semarang Tahun 2014). *Diponegoro Law Journal.* 2016; 5(2): 1-6.

[6] Bagepalli N, Gandhi P, Patra A, Prabhu K, Thakar A, inventors. Cisco Technology Inc, assignee. Highly scalable architecture for application network appliances. United States patent US 9,100,371. 2015.

[7] Kelbert F, Gregor F, Pires R, Köpsell S, Pasin M, Havet A, Schiavoni V, Felber P, Fetzer C, Pietzuch P. *Secure Cloud: secure big data processing in untrusted clouds.* Proceeding of the Conference on Design, Automation & Test in Europe. European Design and Automation Association. 2017: 282-285.

[8] Hoque N, Bhuyan MH, Baishya RC, Bhattacharyya DK, Kalita JK. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications.* 2014; 40: 307-324.

[9] Swildens ES, Liu Z, Day RD, inventors. Akamai Technologies Inc, assignee. Method and system for handling computer network attacks. United States patent US 8,612,564. 2013.

[10] Han SW, Kwon H, Hahn C, Koo D, Hur J. *A survey on MITM and its countermeasures in the TLS handshake protocol.* Proceedings of 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN). IEEE. 2016; 724-729.

[11] Wang X, Gao N, Zhang L, Liu Z, Wang L. *Novel mitm attacks on security protocols in sdn: A feasibility study.* Proceedings of International Conference on Information and Communications Security. Springer, Cham. 2016: 455-465.

[12] SU, Zhendong; WASSERMANN, Gary. *The essence of command injection attacks in web applications.* In: Acm Sigplan Notices. ACM, 2006: 372-382.

[13] Osanaiye O, Choo KK, Dlodlo M. Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications.* 2016; 67: 147-165.

[14] Somani G, Gaur MS, Sanghi D, Conti M, Buyya R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications.* 2017; 107: 30-48.

[15] Gupta S, Gupta BB. Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management.* 2017; 8(1): 512-30.

[16] Gupta S, Gupta BB. Smart XSS attack surveillance system for OSN in virtualized intelligence network of nodes of fog computing. *International Journal of Web Services Research (IJWSR).* 2017; 14(4): 1-32.

[17] Som S, Sinha S, Kataria R. Study on sql injection attacks: Mode detection and prevention. *International Journal of Engineering Applied Sciences and Technology*, Indexed in Google Scholar, ISI etc., Impact Factor: 1.494. 2016; 1(8): 23-29.

[18] Gupta A, Yadav DS. An Approach for Preventing SQL Injection Attack on Web Application. *International Journal of Computer Science and Mobile Computing (IJCSMC)*. 2016; 5(6): 01-10.

[19] Tutt T, Sherwood JR, inventors; Bogart Associates Inc Of Northern Virginia, Bogart Associates, assignee. System and method for secure end-to-end chat system. United States patent US 9,432,340. 2016.

[20] Karabey I, Akman G. *A cryptographic approach for secure client-server chat application using public key infrastructure (PKI).* Proceedings of 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE. 2016; 442-446.

[21] Antenor RA, Bautista R, Lesaca FP, Valencia R. LAF Chat: A Message Encrypting Application Utilizing RSA Algorithm for Android-Based Mobile Device. *TNI Journal of Engineering and Technology.* 2018; 6(1): 24-30.

[22] Natanael D, Suryani D. Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC). *Procedia Computer Science.* 2018; 135: 283-291.

[23] Rehman MM, Akter T, Rahman A. Development of Cryptography-Based Secure Messaging System. *Journal of Telecommunications Systems & Management.* 2016.

[24] Sutikno T, et al. WhatsApp, viber and telegram: Which is the best for instant messaging?. *International Journal of Electrical & Computer Engineering* (2088-8708). 2016; 6(3).

[25] Paim SG, De Rezende WF. *Method for using smartphones as public and personal security devices based on trusted social networks.* U.S. Patent Application No 13/208,710. 2013.

[26] Chalons C, Dufft N. *The role of IT as an enabler of digital transformation.* Proceedings of the drivers of digital transformation. Springer. Cham. 2017: 13-22.

[27] Ermoshina K, Musiani F, Halpin H. *End-to-end encrypted messaging protocols: An overview.* Proceedings of International Conference on Internet Science. Springer. Cham. 2016: 244-254.

[28] Alwen J, Coretti S, Dodis Y. *The double ratchet: security notions, proofs, and modularization for the signal protocol.* Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer. Cham. 2019 May 19: 129-158.

[29] Perrin T, Marlinspike M. The double ratchet algorithm. GitHub wiki. 2016.