Journal of Scientech Research and Development
Volume 3, Issue 1, June 2021
P-ISSN: 2715-6974 E-ISSN: 2715-5846
Open Access at: http://idm.or.id/JSCR

PERANCANGAN APLIKASI ENKRIPSI DATA PESAN SINGKAT DENGAN MENGGUNAKAN ALGORITMA ELGAMAL BERBASIS ANDROID

THE DESIGN OF SHORT MESSAGE DATA ENCRYPTION APPLICATION USING ANDROID-BASED ELGAMAL ALGORITHM

Samsir[1], Danyl Mallisza[2]
Universitas Al Washliyah Labuhanbatu[1]
Program Diploma III Manajemen Informatika Fakultas Ekonomi Universitas Ekasakti[2]
E-mail: samsirst111@gmail.com

INFO ARTIKEL

Koresponden

Samsir
samsirst111@gmail.com

Kata kunci:

Enkripsi, pesan singkat, algoritma elgamal, android, kriptografi

Website:
http://idm.or.id/JSCR

hal: 52 - 62

ABSTRAK

Penelitian ini bertujuan untuk merancang dan membuat sebuah aplikasi untuk keamanan pesan. Kriptografi merupakan bidang ilmu untuk menjaga keamanan pesan (message). Kriptografi telah banyak diimplementasikan di banyak hal. Diantaranya Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan dan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Dengan kata lain kriptografi melakukan penyandian terhadap teks asli (plaintext) menjadi teks sandi (chippertext). Untuk melakukan penyandian sebuah pesan asli menjadi pesan sandi (enkripsi) atau mengubah kembali pesan sandi menjadi pesan asli (dekripsi) diperlukan kunci rahasia. Salah satu sistem kriptografi adalah Sistem Kriptografi Elgamal. Sistem Kriptografi Elgamal merupakan sistem kriptografi dengan kunci asimetri, dimana kunci untuk mengenkripsi dan mendekripsi adalah berbeda.

ARTICLE INFO

Correspondent:

Samsir
samsirst111@gmail.com

Key words:

encryption, short massage, elgamal algorithm, android, cryptography

Website:
http://idm.or.id/JSCR

page: 63 - 73

ABSTRACT

This study aimed to design and create an application for message security. Cryptography is a field of science to maintain the security of messages (message). It has been widely implemented in many ways. Among Smart cards, Automated Teller Machine (ATM), Pay TV, Mobile Phones, and Computers are a few examples of products that use cryptographic technology to its safety. Cryptography is the science that relied on mathematical techniques for dealing with security and information such as confidentiality, integrity and authentication of data entities. In other words, perform cryptographic encryption of the original text (plaintext) into ciphertext (chippertext). To perform encoding an original message into a coded message (encryption) or change the password messages back into the original message (decryption) required a secret key. One cryptosystem is the ElGamal Cryptography System. Cryptography ElGamal system is a key crypto systems with asymmetry, where the key to encrypt and decrypt are different

PENDAHULUAN

Perkembangan teknologi pada zaman sekarang ini begitu cepat, khusus teknologi informasi salah satunya telepon seluler, fitur dan kecanggihannya pada telepon seluler mulai muncul sampai dengan adanya yang disebut smartphone, yang memiliki berbagai fungsi seperti multimedia, multiplayer games, transfer data, video streaming dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan diantaranya yang cukup dikenal luar adalah pada platform smartphone khususnya Android.

Salah satu fasilitas yang disediakan ponsel adalah untuk melakukan pegiriman data berupa pesan singkat melalui Short Message Service (SMS). Namun dengan fasilitas SMS yang ada, sering muncul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu informasi rahasia melalui fasilitas SMS. Kriptografi merupakan bidang ilmu untuk menjaga keamanan pesan (*message*). Kriptografi telah banyak diimplementasikan di banyak hal. Diantaranya *Smart card*, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya.

Dalam kriptografi terdapat metode yang cukup penting dalam pengamanan data, yaitu dengan metode ElGamal untuk mengekripsi data yang berjalan pada sistem operasi Android sehingga pemilik telepon seluler yang berbasis android dapat melakukan pertukuran data SMS dengan lebih aman dan nyaman. Dalam menjaga kerahasian SMS, dibutuhkan suatu cara untuk mengamankan informasi yang sifatnya penting atau rahasia, yaitu dengan melakukan enkripsi terhadap teks SMS maka tingkat kemanan informasi dari pesan tersebut dapat ditingkatkan.

METODE PENELITIAN

Studi Kepustakaan (*Library Research*)

Yaitu dengan cara memperoleh data dengan menggunakan buku-buku yang relevan berhubungan dengan masalah yang dihadapi dalam pembuatan alat, teknik penggunaan komponen, teknik penggunaan alat dengan maksud untuk mendapatkan data yang tepat.

Internet (*Surfing*)

memperoleh data dari situs-situs internet yang berhubungan dengan masalah yang sedang dibahas dan men-download-nya sebagai bahan referensi. Dalam hal ini dokumentasi-dokumentasi, FAQ (*Frequently Asked Questions*), RFC (Request for *Comments*) dan *How to Manual* yang terdapat pada situs-situs yang berhubungan dengan masalah yang sedang dibahas.

Pengujian

Langkah terakhir dilakukan pengujian alat yang dibuat, apakah sudah sesuai dengan sistem yang sudah diharapkan.

HASIL DAN PEMBAHASAN

Proses uji coba dari aplikasi ini dengan melakukan pengujian langsung terhadap pesan yang akan dienkripsi maupun didekripsi. Pada pembuatan aplikasi ini dibuat keamanan sistem data SMS yang mana dalam program ini pesan yang akan dikirim terenkripsi dengan menggunakan algoritma yang sudah ditentukan.

Pada umumnya orang mengirim pesan tanpa menggunakan enkripsi, jadi pada pengiriman pesan bisa dihacker atau diseludupi orang yang tidak bertanggung jawab. Oleh karena itu, dibuat perancangan aplikasi enkripsi data pesan singkat dengan menggunakan algoritma ElGamal berbasis android, yang mana program ini dibuat dengan sebaik mungkin.

Dengan adanya program ini menambah keamanan dalam mengirim pesan yang rahasia kepada kepada penerima tanpa diketahui oleh orang lain. Aplikasi ini sangat mudah dipahami dan dipelajari dan aplikasi ini bisa dijalankan didalam *Smartphone*.

Tampilan Layar

Pada bagian ini merupakan penjelasan dari hasil rancangan interface untuk administrator yang terdiri dari sebagai berikut:

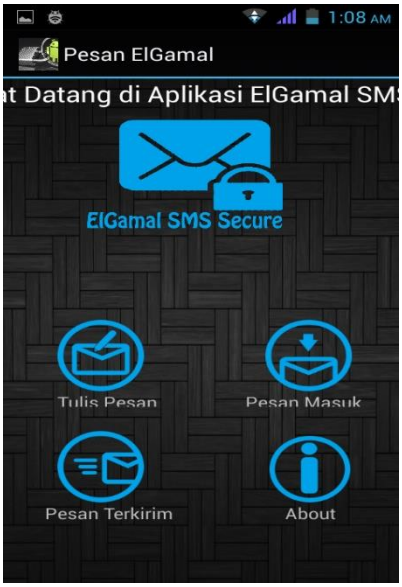
1. Interface Splash

Adapun hasil dari rancangan interface splash dapat dilihat pada gambar 1 dibawah ini.

Gambar 1. *Interface Splash*

2. ***Interface*** **Menu Utama**

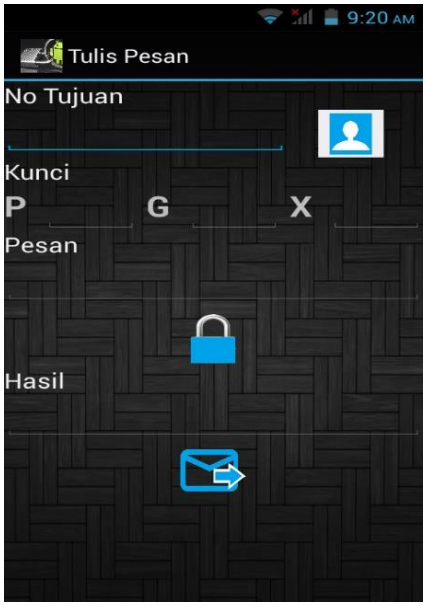
Pada interface menu ini menampilkan form yang disediakan untuk pengguna mengakses sistem atau untuk menjalankan aplikasi yang telah dirancang, dimana pada menu terdapat form-form yang mempunyai fungsi masing-masing. Adapun interface menu dapat dilihat pada gambar 2 berikut ini.



Gambar 2. *Interface Menu Utama*

3. Interface Menu

Pada interface menu ini menampilkan form yang disediakan untuk pengguna menjalankan aplikasi pesan yang telah dirancang, dimana pada menu terdapat fungsi mengenkripsi pesan dan mengirim pesan. Adapun interface menu dapat dilihat pada Gambar 3 berikut ini.



Gambar 3. *Interface* Menu Tulis Pesan

Pada desain menu tulis pesan di aplikasi untuk keamanan data pesan singkat ini dapat dijelaskan sebagai berikut:

a. No tujuan, berfungsi untuk memasukkan no.
b. Kontak, berfungsi untuk mengambil no tujuan dari penyimpanan no.
c. Kunci p, g, berfungsi untuk menginputkan kunci publik untuk melakukkan enkripsi pesan.
d. Kunci x, berfungsi untuk menginput kunci privat sebelum melakukan enkripsi pesan.
e. Pesan, berfungsi untuk memasukkan pesan yang akan di enkripsi.
f. Tombol enkripsi, berfungsi untuk memproses enkripsi pesan.
g. Hasil, berfungsi untuk menampilkan hasil proses dari enkripsi pesan.
h. Tombol kirim, berfungsi untuk mengirimkan pesan.

4. Interface Form Hasil Enkripsi

Interface ini merupakan form setelah proses enkripsi pesan berjalan lancar. Adapun interface form hasil enkripsi dapat dilihat pada Gambar 4 berikut ini.

Gambar 4. *Interface Form* **Hasil** *Enkripsi*

5. Interface Form Hasil Dekripsi

Interface ini merupakan form setelah proses dekripsi pesan berjalan. Adapun interface form hasil dekripsi dapat dilihat pada Gambar 5 berikut ini.

Gambar 5. Interface Form Hasil Dekripsi

BlackBox

Pengujian blackbox (blackbox testing) adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas. Tahap pengujian atau testing merupakan salah satu tahap yang harus ada dalam sebuah siklus pengembangan perangkat lunak (selain tahap perancangan atau desain). Berikut pengujian sistem dengan metode blackbox testing yang disajikan pada tabel pengujian blackbox seperti dibawah ini.

Tabel 1. Hasil Pengujian Black Box Aplikasi Enkripsi Teks Menggunakan Algoritma Elgamal

No	Form	Keterangan	Hasil
1	Masuk ke aplikasi ElGamal	Sistem akan membuka aplikasi menampilkan layar pembuka aplikasi dan menuju menu pilihan	Valid
2	Memilih menu tulis pesan	Akan membuka form tulis pesan	Valid
3	Klik tulis pesan, no. tujuan, masukan Key, enkripsi pesan dan kirim sms	Menghasilakan plainteks yang tersimpan di kotak masuk	Valid
4	Lanjut proses dekripsi dengan melihat kotak masuk dan masukan key klik hasil	Menghasilkan chiperteks yang telah di dekripsi	Valid
5	Melihat pesan terkirim	Akan tampil hasil yang telah di kirim	Valid
6	Memilih menu *about*	Akan tampil menu *About*	Valid

Untuk menjalankan program ini dibutuhkan perangkat keras (hardware) sebagai berikut:

1. Prosesor Intel Core i3 atau diatasnya
2. RAM dengan kapasitas 2Gb
3. Keyboard, Mouse
4. Android Mobile Phone

Sedangkan perangkat Lunak (Software) yang dibutuhkan:

1. SDK Java sebagai mesin aplikasi Java pada aplikasi desktop
2. Sistem operasi android pada mobile phone
3. Wifi ADB dari playstore

Analisa Hasil

Prosedur pembangkitan kunci sistem kriptografi elgamal adalah sebagai berikut:

1. Kunci publik pertama (p) merupakan bilangan prima lebih besar dari 255.
2. Kunci privat (x) didapat dengan cara menentukan secara acak dari bilangan 1 hingga $p - 2$.
3. Kunci publik kedua (g) merupakan bilangan yang dimulai dari 2,3,4,5 dan seterusnya hingga hasil perhitungan $g^{((p-1)/2)} \bmod p$ tidak sama dengan 1.
4. Kunci publik ketiga (y) merupakan hasil perhitungan dengan rumus $y = g^x \bmod p$.

Tabel 2. Pasangan Kunci Sistem Kriptografi ElGamal

Kunci Publik P	Kunci Publik G	Kunci Privat X
2903	6	11
863	5	373
911	7	199
719	11	631
2909	7	13

Hasil Uji Coba Enkripsi

Berikut ini adalah tabel hasil pengujian enkripsi pesan karakter dengan menggunakan kunci publik P = 2903, G = 6, dan kunci privat X = 11.

Tabel 3. Hasil Pengujian Enkripsi

No	Karakter	Desimal	k	C1=G^k Mod P	C2=Y^k m Mod P
1.	M	117	784	2209	2646
2.	e	116	2315	834	1341
3.	d	97	826	2421	383
4.	a	109	422	2168	2869
5.	n	97	2806	1205	2614

Hasil Uji Coba Dekripsi

Berikut ini adalah tabel hasil pengujian dekripsi pesan karakter dengan menggunakan kunci publik P = 2903 kunci privat X = 11.

Tabel 4. Hasil Pengujian Dekripsi

No	C1	C2	D={$C1^{p-x-1}$. C2} Mod P	Karakter
1.	2209	2646	77	M
2.	834	1341	101	e
3.	2421	383	100	d
4.	2168	2869	97	a
5.	1205	2614	110	n

Kelebihan Dan Kekurangan

Kelebihan aplikasi yang dirancang adalah sebagai berikut:

1. Aplikasi dapat menjaga keamanan dan kerahasiaan pesan dari orang yang tidak bertanggung jawab.
2. Aplikasi ini bekerja dengan kombinasi dari tiga kunci publik dan satu kunci privat yang merupakan bilangan prima.
3. Mempermudah user dalam mengamankan data.
4. Mudah digunakan karena user interface yang sederhana

Sedangakan sebagai kekurangan aplikasi yang dirancang adalah sebagai berikut:

1. Tampilan dan layout dari aplikasi masih sederhana.
2. Proses enkripsi hanya bisa dilakukan pada pesan karakter saja, tidak bisa file audio, gambar dan video.
3. Biaya untuk kirim pesan yang telah di enkripsi menjadi Chipertext akan lebih besar, karena panjang hasil enkripsi pesan menjadi dua kali lipat dari sebelumnya.
4. Ketika mengenkripsi pesan dengan jumlah karakter yang terlalu panjang akan memakan waktu yang cukup lama.

SIMPULAN DAN SARAN

Simpulan

1. Penerapan algoritma kriptografi elgamal pada program yang telah dibuat adalah sesuai dengan proses algoritma kriptografi elgamal yang ada. Hal ini dibuktikan dengan terbentuknya pasangan kunci publik dan kunci privat.
2. Kunci publik yang dihasilkan terdiri dari tiga buah bilangan yaitu nilai p,g dan y dan kunci privat hanya satu yaitu nilai x.
3. Hasil enkripsi yang dihasilkan memiliki panjang dua kali lipat dari panjang plaintext awal. Hal ini dikarenakan setiap blok plaintext dienkripsi dengan

mencari pasangan *chipertext* $a = g^k \bmod p$ dan $b = y^k m \bmod p$. Sehingga menghasilkan pasangan (a,b).

4. Algoritma kriptografi elgamal dapat diterapkan pada bahasa pemrogram java untuk pengamanan pesan.

Saran

1. Perlu dilakukan pengembangan atau perbaikan pada desain interface agar lebih memudahkan pengguna dalam menggukan aplikasi ini.
2. Jenis file yang dapat diekripsi hendaknya bukan hanya file teks saja tetapi mencakup beberapa file seperti file gambar, video atau suara.
3. Perlunya dilakukan kombinasi dari dua atau lebih algoritma kriptografi agar lebih menjamin tingat keamanan data.

DAFTAR PUSTAKA

Syaiful Zuhri Harahap and Samsir, "Application Design The Data Collection Features of The Hotel Shades of Rantauprapat Using VBNET," *Int. J. Sci. Technol. Manag.*, vol. 1, no. 1, pp. 1–6, 2020, doi: 10.46729/ijstm.v1i1.4.

Z. Zulkifli and S. Samsir, "Implementasi Sistem Keamanan SQL Injection Dalam berbasis web," *U-NET Tek. Inform.*, vol. 04, no. 01, pp. 13–17, 2020.

D. Indra *et al.*, "SPK Untuk Pemilihan Kepala Sekolah Menggunakan Metode Saw dan Profile Matching," vol. 4, no. 1, pp. 7–12, 2020.

J. H. P. Sitorus *et al.*, "Perancangan pengontrol lampu rumah miniatur dengan menggunakan micro controler arduino berbasis android 1," vol. 4, no. 1, pp. 1–11, 2020.

M. V. B. Net, "PADA TOKO URIP MOTOR," no. September, pp. 1–6, 2020.

U. Verawardina, F. Edi, and R. Watrianthos, "Analisis Sentimen Pembelajaran Daring Pada Twitter di Masa Pandemi COVID-19 Menggunakan Metode Naïve Bayes," vol. 5, pp. 157–163, 2021, doi: 10.30865/mib.v5i1.2604.

Samsir, "Perancangan Aplikasi Sistem Pendukung Keputusan Penentuan Beasiswa Di SMK Raudlatul Ulum Aek Nabara Dengan Metode Simple Additive Weighting Berbasis Web," *U-NET J. Tek. Inform.*, vol. 3, no. 1, pp. 21–27, 2019, doi: 10.52332/u-net.v3i1.18.

W. Fahrozi, "Penerapan Analytical Network Process Dalam Menentukan Ras Ayam Serama Simple Additive Weighting (SAW)," vol. 03, no. 01, pp. 28–34, 2019, doi: 10.52332/u-net.v3i1.19.

A. Syahputra, D. I. G. Hts, and Samsir, "Perancangan Aplikasi Media Pembelajaran Jarimatika Penjumlahan Dan Pengurangan Berbasis Multimedia," *U-NET J. Tek. Inform.*, vol. 3, no. 1, pp. 35–42, 2019, doi: 10.52332/u-net.v3i1.20.

Samsir, D. I. Gunawan HTS, and S. Z. Harahap, "Sistem Pendukung Keputusan Pemilihan Kepala Sekolah Menggunakan Metode Saw dan Profile Matching," *U-NET J. Tek. Inform.*, vol. 4, no. 1, pp. 1–7, 2020, doi: 10.52332/u-net.v4i1.162.

Zulkifli and Samsir, "Implementasi Sistem Keamanan SQL Injection Dalam berbasis web," *U-NET J. Tek. Inform.*, vol. 4, no. 1, pp. 8–13, 2020, doi: 10.52332/u-net.v4i1.164.

Zulkifli, Samsir, and Azrai Sirait, "Implementasi Max Length dan Input Type Number Pada Form Login Website Untuk Mencegah Penetrasi SQL Injeksi Secara Paksa," *U-NET J. Tek. Inform.*, vol. 4, no. 1, pp. 14–18, 2021, doi: 10.52332/u-net.v4i1.223.

S. P. Sitorus and S. Samsir, "Perancangan Aplikasi Game Tetris Batu Bara," *U-NET J. Tek. Inform.*, vol. 3, no. 2, pp. 35–41, 2019, doi: 10.52332/u-net.v3i2.290.

Firman Edi, A. Ambiyar, U. Verawardina, S. Samsir, and R. Watrianthos, "Improving Lesson Plan Models Using Online-Based in the New Normal Era," *EDUTEC J. Educ. Technol.*, vol. 4, no. 3, pp. 527–535, 2021, doi: 10.29062/edu.v4i3.109.

R. A. Purba, S. Samsir, M. Siddik, S. Sondang, and M. F. Nasir, "The optimalization of backpropagation neural networks to simplify decision making," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 830, no. 2, 2020, doi: 10.1088/1757-899X/830/2/022091.

S. Samsir, S. Suparno, and M. Giatman, "Predicting the loan risk towards new customer applying data mining using nearest neighbor algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 830, no. 3, 2020, doi: 10.1088/1757-899X/830/3/032004.

Samsir, F. Edi, K. Ginting, S. Hartati, Sondang, and R. A. Purba, "Edge Detection to Make Drawing Sketch using Laplacian Operator and Gabor Wavelet for Learning Devices," *J. Phys. Conf. Ser.*, vol. 1764, no. 1, 2021, doi: 10.1088/1742-6596/1764/1/012070.

S. Samsir, J. H. P. Sitorus, Zulkifli, Z. Ritonga, F. A. Nasution, and R. Watrianthos, "Comparison of machine learning algorithms for chest X-ray image COVID-19 classification," *J. Phys. Conf. Ser.*, vol. 1933, no. 1, p. 012040, 2021, doi: 10.1088/1742-6596/1933/1/012040.

M. P. Covid-, "Analisis Sentimen Pembelajaran Daring Pada Twitter," vol. 5, pp. 174–179, 2021, doi: 10.30865/mib.v5i1.2293.

Samsir and Syaiful Zuhri Harahap, "Application Design Resume Medical By Using Microsoft Visual Basic. Net 2010 At the Health Center Appointments," *Int. J. Sci. Technol. Manag.*, vol. 1, no. 1, pp. 14–20, 2020, doi: 10.46729/ijstm.v1i1.5.

W. Fahrozi, P. T. Informatika, T. Informatika, F. U. A. Labuhanbatu, T. Mulia, and K. Medan, "U-NET : Jurnal Teknik Informatika LPPM – Universitas Al Washliyah Labuhanbatu 23 | P a g e U-NET : Jurnal Teknik Informatika Sebagai langkah awal yang dilakukan supaya dapat mengetahui gambaran permasalahan yang dihadapi dalam menentukan rasa yam serama a," vol. 3, no. 5, pp. 23–27, 2019.

M. Siddik and S. Samsir, "Rancang Bangun Sistem Informasi Pos (Point of Sale) Untuk Kasir Menggunakan Konsep Bahasa Pemrograman Orientasi Objek," *JOISIE (Journal Inf. Syst. Informatics Eng.*, vol. 4, no. 1, p. 43, 2020, doi: 10.35145/joisie.v4i1.607.

P. T. Informatika and F. U. A. Labuhanbatu, "U-NET : Jurnal Teknik Informatika LPPM – Universitas Al Washliyah Labuhanbatu 18 | P a g e U-NET : Jurnal Teknik Informatika Sebagai langkah awal yang dilakukan supaya dapat mengetahui gambaran permasalahan yang dihadapi oleh bagian kesiswaan adalah denga," vol. 3, no. 4, pp. 18–22, 2019.

Samsir, "Klasifikasi Penyakit Tenggorokan Hidung Telinga (THT) Menggunakan Jaringan Syaraf Tiruan Dengan Metode Learning Vektor Quantization (THT) Di RSUD Rantauprapat Labuhanbatu Klasifikasi penyakit Tenggorokan Hidung Telinga (THT) Menggunakan," vol. 05, no. 01, pp. 38–47, 2019.

D. I. G. H. Wirhan Fahrozi, Samsir, "Penerapan E-Commerce Pada Toko Bunga Underwear," *J. Tek. Inform.*, vol. 04, no. 01, pp. 1–6, 2020.

F. Edi, P. T. Informatika, and F. U. A. Labuhanbatu, "UNET | Jurnal Ilmiah Teknik Informatika LPPM Universitas Al Washliyah Labuhanbatu UNET | Jurnal Ilmiah Teknik Informatika ISSN . 2460-3694 , Vol . 2 No . 1 Februari 2018," vol. 2, no. 1, pp. 2–5, 2018.