JEAT: Journal of Electrical and Automation Technology e-ISSN: 2830-0939
VOL.2, No.2, Desember 2023, hal. 90-96

IMPLEMENTATION OF BCRYPT ALGORITHM FOR SIPAPEDA WEBSITE SECURITY AT BAPPEDA OFFICE, BUTON REGENCY WITH ONE TIME PASSWORD METHOD

Jabal Nur[1], Azlin*[2]
[1,2] Program Studi Teknik Informatika Universitas Dayanu Ikhsanuddin
e-mail: [1]jabalnur@unidayan.ac.id, [2]azlin.unidayan01@gmail.com*

Abstract

The Office of the Regional Development Planning Agency (BAPPEDA) of Buton Regency has a website, namely the Regional Development Design Data Processing Information System (SIPAPEDA) where the SIPAPEDA Website is used to input data as well as an information system from each office in Buton Regency. With the large number of users of the Website, the security on the Website must be improved. Based on these problems, the security of the SIPAPEDA website is improved by using the Bcrypt algorithm and using One Time Password (OTP) as verification at login. With the aim of securing the Sipapeda Website of Buton Regency using the Bcrypt Algorithm with the One Time Password (OTP) Authentication Method. In this study using data collection methods, namely observations, interviews and literature and data analysis that refers to the types of data and data sources. This study resulted in the Sipapeda website being able to increase its security using the Bcrypt algorithm, as well as security in the login process requiring OnTime Password verification.

Keyword*: Security, Cryptographi, Bcrypt*

Abstrak

Kantor Badan Perancangan Pembangunan Daerah (BAPPEDA) Kabupaten Buton memiliki sebuah Website yaitu Sistem Informasi Pengolahan Data Perancangan Pembangunan Daerah (SIPAPEDA) dimana Website SIPAPEDA digunakan untuk menginput data sekaligus sebagai Sistem Informasi dari tiap-tiap Kantor yang ada di Kabupaten Buton. Dengan banyanknya pengguna Website tersebut maka keamanan pada Website tersebut harus ditingkatkan. Berdasarkan masalah tersebut maka keamanan website SIPAPEDA ditingkatkan dengan menggunakan algoritma Bcrypt serta menggunakan One Time Password (OTP) sebagai verifikasi pada saat login. Dengan tujuan untuk mengamankan Website Sipapeda Kabupaten Buton menggunakan Algoritma Bcrypt dengan Metode Autentikasi One Time Password (OTP). Dalam penelitian ini menggunakan metode pengumpulan data yaitu pengamatan (Observasi), wawancara dan kepustakaan serta analisis data yang merujuk pada jenis data dan sumber data. Penelitian ini menghasilkan website Sipapeda dapat ditingkatkan keamanannya menggunakan algoritma Bcrypt, serta keamanan pada proses login membutuhkan verifikasi On Time Password.

Kata kunci: Keamanan, Kriptografi, Bcrypt

1. Pendahuluan

Kantor Badan Perancangan Pembangunan Daerah (BAPPEDA) Kabupaten Buton memiliki sebuah Website yaitu sistem informasi pengolahan data perancangan pembangunan daerah (SIPAPEDA) dimana Website tersebut dibuat karena sulitnya Kantor BAPPEDA untuk mendapatkan data dari tiap-tiap dinas yang dimana data dari tiap dinas didapat harus melalui operator tiap-tiap dinas. Website SIPAPEDA digunakan untuk menginput data sekaligus sebagai Sistem Informasi dari tiap-tiap kantor yang ada di Kabupaten Buton. Dengan banyanknya pengguna Website tersebut maka keamanan pada Website tersebut harus ditingkatkan agar data yang ada pada Website dapat terjaga untuk menghindari pencurian data.

Beberapa penelitian terkait yaitu analisis kinerja algoritma Bcrypt untuk meningkatkan keamanan password dari Brute Force. Tujuan dari penelitian ini yaitu menghasilkan keamanan password dari serangan Brute Force dengan algoritma Bcrypt. Kesimpulan dari penelitian ini

adalah hasil kinerja algoritma Bcrypt cukup baik dalam menangkal serangan Brute Force pada karakter abjad dan campuran sedangkan untuk karakter angka Bcrypt tidak cukup baik dalam menangkal serangan Brute Force[1].

Penelitian lainnya yaitu dengan judul implementasi metode autentikasi one time password (OTP) berbasis mobile token pada aplikasi ujian online. Tujuan penilitian ini yaitu untuk memperkecil bahkan kalau bisa meniadakan kemungkinan untuk akses ilegal ketika melakukan proses ujian online. Kesimpulan penelitian ini yaitu Penerapan Metode Autentikasi One Time Password (OTP) dapat meningkatkan keamanan proses autentikasi. PIN/OTP yang dikirim melalui jaringan bukanlah PIN/OTP yang signifikan dan selalu berubah-ubah setiap kali dibangkitkan, sehingga menjadi lebih sulit untuk membajak sesi autentiksi pada setiap waktu [2].

Penelitian lainnya dengan judul aplikasi mobile one time password menggunakan algoritma Md5 dan Sha1 untuk meningkatkan keamanan website. Tujuan dari penelitian ini yaitu untuk mencegah hal-hal yang tidak diinginkan pada Sistem Informasi. Kesimpulan dari penelitian ini yaitu Algoritma SHA1 dan MD5 digunakan pada penerapan One Time Password dapat mengamankan login website, menggunakan Smartphone Android untuk mengimplementasikan One Time Password, dan juga menggunakan algoritma MD5 dan SHA1 untuk meningkatkan keamanan informasi pada website[3].

Penelitian lainnya yaitu Analisis Keamanan Sistem Login. Tujuan penelitian ini yaitu untuk mendeteksi suatu password yang berhasil di enkripsi dan tidak di enkripsi. Kesimpulan dari penelitian ini yaitu Pentingnnya memperhatikan pengamanan password pada sistem login sebelum dikirim ke server[4].

Penelitian lainnya yaitu Faktor-Faktor Yang Mempengaruhi Kualitas Layanan Website Bank Syariah Terhadap Perolehan Informasi Nasabah (Studi BNI Syariah Kota Bogor). Tujuan penelitian ini yaitu untuk mengetahui faktor-faktor yang paling dominan mempengaruhi kualitas layanan Website BNI syariah untuk memperoleh informasi nasabah di Bogor. Kesimpulan dari penelitian ini yaitu Faktor utama yang mempengaruhi kualitas layanan Website BNI Syariah terhadap perolehan informasi nasabah di Kota Bogor pada penelitian ini adalah relevan dengan nilai 0,841, aksesibilitas dengan nilai 0,835, konten dengan nilai 0,742, sistem navigasi dengan nilai 0,696 dan kepercayaan dengan nilai 0,685[5].

Penelitian lainnya yaitu Implementasi Keamanan Login Dengan Metode One Time Password (OTP) Menggunakan Fungsi Hash Algoritma Sha-512 Pada SMP Negeri 3 Tangerang Selatan. Tujuan dari penelitian ini yaitu untuk mengamankan sistem login tersebut dibutuhkan lapisan keamanan berlapis salah satunya seperti penggunaan kode OTP untuk verifikasi sementara dan hanya bisa diakses oleh penggunanya itu sendiri sehingga bisa mengurangi potensi penyadapan hak akses. Adapun kesimpulan dari penelitian yaitu dengan menggunakan metode OTP dapat meningkatkan keamanan penggunaan kata sandi pada saat proses login agar menjaga dari serangan phishing[6].

Penelitian lainnya yaitu Implementasi Algoritma Md5 Untuk Keamanan Dokumen. Tujuan dari penelitian ini yaitu untuk melakukan proses enkripsi dan dekripsinya sehingga akan dihasilkan dokumen yang sama dengan dokumen aslinya. Kesimpulan dari penelitian ini yaitu Algoitma kriptografi MD5 dengan kemampuan enkripsi yang dimiliki dapat menjadi rekomendasi untuk keamanan data dan jaringan sistem computer[7].

Peningkatan lainnya dengan judul Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia adalah penelitian dari tables (Musliyana, Z., Arif, T. Y., Munadi, R., & Sarjana, P, 2016) yang bertujuan untuk meningkatkan keamanan pada otentikasi Single Sign On (SSO) Universitas Ubudiyah Indonesia. Kesimpulan dari penelitian ini yaitu penerapan algoritma AES dengan pembangkit kunci dinamis pada ontentikasi Single Sign On (SSO) Universitas Ubudiyah Indonesia dapat mencegah serangan dictionary attacks dan rainbow tables[8].

Penelitian lainnya yaitu Algoritma Blowfish Untuk Meningkatkan Keamanan Database Mysql. Tujuan dari penelitian ini yaitu untuk menerapkan algoritma Blowfish sebagai metode untuk meningkatkan keamanan data dalam database MySQL. Kesimpulan dari penelitian ini adalah Algoritma Blowfish pun dapat digabungkan dengan algoritma-algoritma enkripsi yang lain dalam pengkripsian sebuah pesan untuk lebih menjamin isi dari pesan, namun dalam hal ini hanya menggunakan algoritma tersebut untuk enkripsi dan dekripsi[9].

Penelitian lainnya dengan judul Aplikasi Absensi Pegawai pada Dinas Komunikasi dan Informatika Kabupaten Deli Serdang dengan QR Code Menggunakan Algoritma Bcrypt . Tujuan

dari penelitian ini adalah untuk mengatasi masalah kecurangan yang mungkin dilakukan berupa URL, nomor telepon, pesan SMS, VCard, atau teks apapun dengan menggunakan teknologi QRCode berbasis web. Kesimpulan dari penelitian ini yaitu aplikasi Absensi dengan memanfaatkan QR Code jauh lebih praktis dan dapat menyimpan informasi secara cepat dengan respon yang cepat, Dapat mempercepat proses perekapan data kehadiran menjadi lebih efektif[10].

2. Metode Penelitian

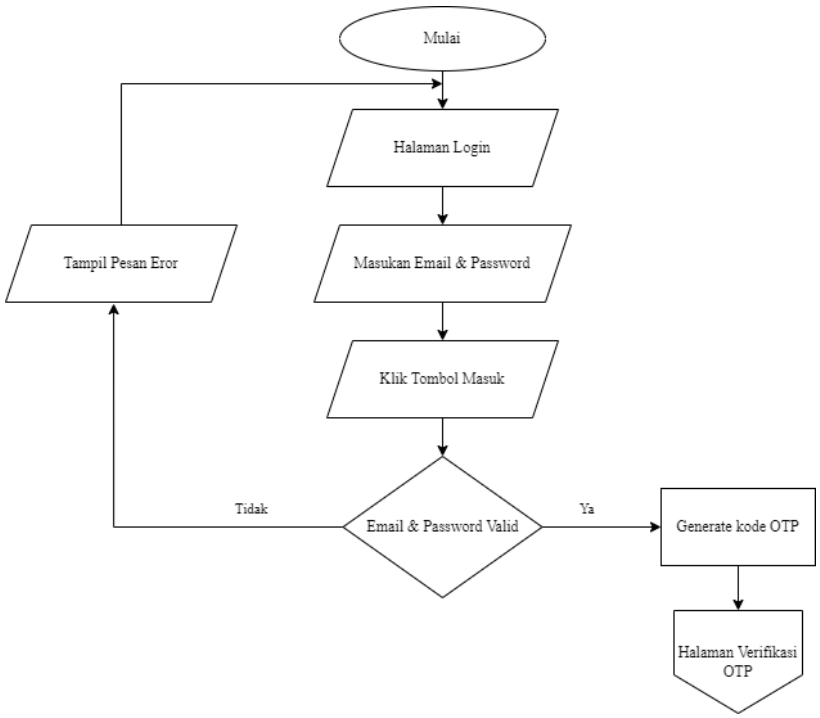
Metode penelitian menjelaskan kronologis penelitian, termasuk desain penelitian, prosedur penelitian (dalam bentuk algoritma, pseudocode atau hal-hal terkait lainnya), cara menguji, dan proses akuisisi data [3], [4]. Setiap deskripsi yang terkait dengan metode penelitian harus didukung oleh referensi.

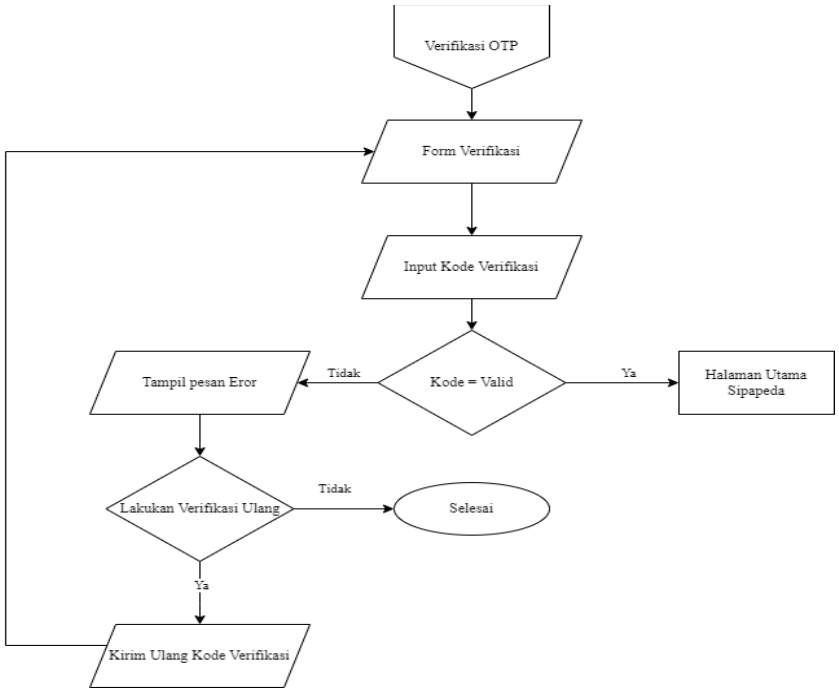
2.1. Tahapan Pengumpulan Data

Cara pengumpulan data yang dilakukan untuk mendapatkan keterangan yang akurat,diperlukan beberapa metode yaitu :

a. Metode Observasi yang dilakukan di kantor BAPPEDA Kabupaten Buton yaitu pada Kantor BAPPEDA Kabupaten Buton memiliki sebuah *website* yaitu Sistem Informasi Pengolahan Data Pembangunan Daerah (SIPAPEDA) yang dimana *website* tersebut berisikan informasi mengenai data yang ada pada tiap-tiap instansi terkait di Kabupaten Buton. *Website* tersebut dibangun menggunakan bahasa pemrograman *PHP* dengan *Framework Laravel* tujuan dibuatnya *website* ini untuk mempermudah pegawai Kantor BAPPEDA Kabupaten Buton dalam hal memperolah data yang di tiap-tiap instansi terkait.
b. Metode wawancara langsung kepada pimpinan instansi yaitu dengan bapak Ahmad Mulia, S.Pt.,M.Si mengenai hal-hal yang berhubungan dengan *Website* SIPAPEDA yang ada pada Kantor BAPPEDA Kabupaten Buton beliau mengatakan bahwa *website* SIPAPEDA ini akan dikembangkan dan akan memuat banyak data dari tiap-tiap instansi terkait.
c. Metode Kepustakaan **(***Library Research)* dilakukan guna untuk mmperoleh referensi terkait sistem keamanan *Website* dari segi metode maupun algoritma, baik itu dalam bentuk buku, jurnal ataupun artikel.

2.1. Flow Chart Aplikasi





Gambar 1 *Flow Chart* Aplikasi

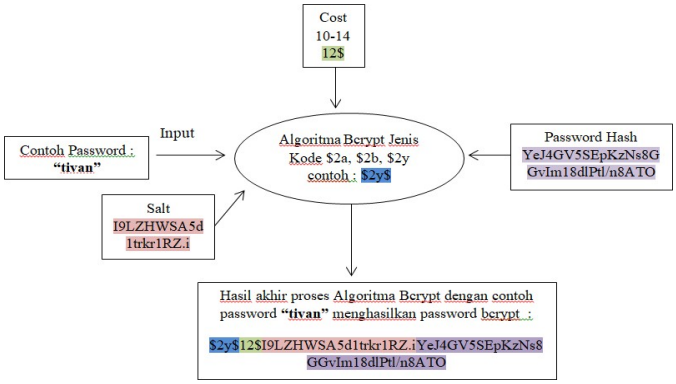
Berikut merupakan penjelasan dari gambar 1 :

1. Masuk kehalaman *login website* sipapeda
2. Masukan *username* dan *pasword* pada halaman *login*
3. Jika *username* dan *password* benar maka system akan mengirimkan kode OTP, jika *username* dan *password* tidak sesuai maka muncul pesan *eror*.
4. Selanjutnya masukan kode OTP yang telah dikirim system, jika kode OTP sesuai maka akan muncul tampilah utama dari aplikasi dan apabila kode OTP salah maka akan muncul pesan eror.

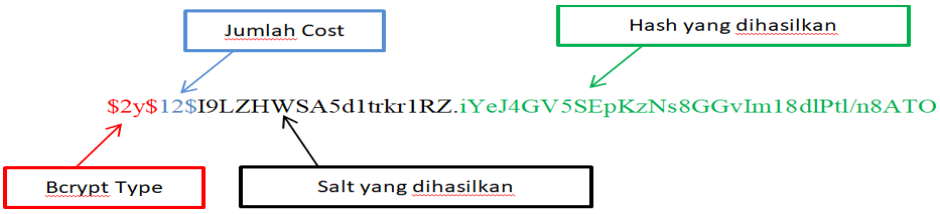
3. Hasil dan diskusi

3.1. Proses Pengamanan Password Menggunakan Algoritma *Bcrypt*

Alur proses pengamanan password menggunakan algoritma bcrypt dapat dilihat gambar berikut :



Gambar 2 Proses Pengamanan Password dengan Algoritma *Bcrypt*



Gambar 3 Hasil dari Proses Algoritma *Bcrypt*

Berikut penjelasan dari proses contoh password yang diamankan *bcrypt* adalah sebagai berikut :

Dari *plaintext* yang diinputkan yaitu “tivan” maka *password bcrypt* yang didapatkan yaitu $2y$12$I9LZHWSA5d1trkr1RZ.iYeJ4GV5SEpKzNs8GGvIm18dlPtl/n8ATO. Keterangan *password* yang dihasilkan diatas adalah :

1. *Bcrypt* = $2y$
   Tipe *bcrypt* yang digunakan pada sistem ini yaitu $2y$ yang merupakan bawaan dari *Framework Laravel*
2. *Cost / Round* = 12
   Cost merupakan banyaknya perputaran atau pengacakan yang dilakukan
3. *Salt* = I9LZHWSA5d1trkr1RZ.i
   Salt merupakan input *random* tambahan yang disimpan dan digunakan untuk emperkuat enkripsi atau *hash* dari sebuah password atau teks. Pada metode ini, digunakan *salt* yang berbeda untuk tiap password, sehingga dihasilkan *hash* yang berbeda dari sebuah *string* yang sama.
4. *Hash* = iYeJ4GV5SEpKzNs8GGvIm18dlPtl/n8ATO
   Hash yang diperoleh merupakan hasil dari *hash* plantext yang telah di acak dan disimbolkan dengan *base -64*

3.2. Tampilan Aplikasi

3.2.1. Halaman Login

Gambar 4. Halaman Login

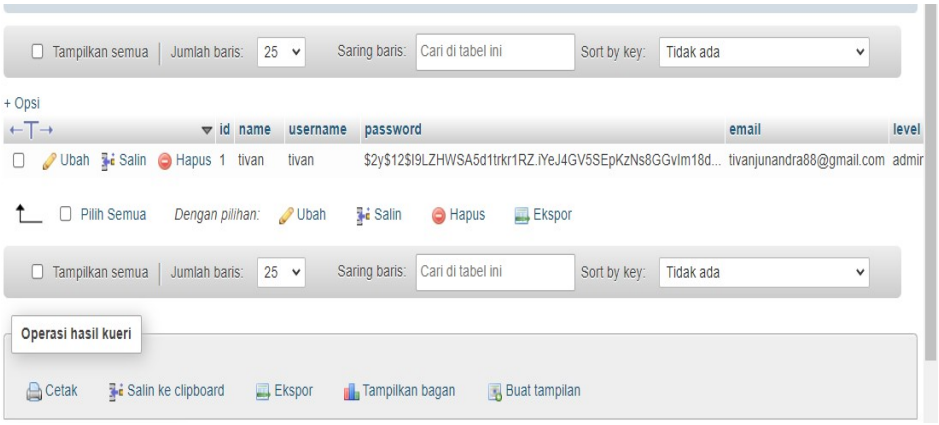
Halaman login berfungsi untuk melakukan penginputan username dan password sebelum masuk ke aplikasi yang dimana username dan password dapat berupa huruf, angka, simbol ataupun kombinasi dari ketiganya.

3.2.2. Halaman Pesan Verifikasi Email

Gambar 5. Halaman Pesan Verifikasi Email

Halaman pesan verifikasi email berisikan informasi yang berupa kode verifikasi yang dikirim ke email pengguna dimana kode tersebut dikirim oleh admin dengan kombinasi kode huruf dan angka.

3.2.3. Penerapan Algoritma Bcrypt Pada Data Base Login



Gambar 6. Penerapan Algoritma Bcrypt Pada Data Base Login

Gambar 6. Menggambarkan penerapan *algoritma Bcrypt* pada tabel Login dimana untuk Password dalam *database* dienkripsi.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan dengan judul implementasi *algoritma bcrypt* untuk keamanan website sipapeda kantor bappeda kabupaten buton dengan metode *one time password*, dapat ditarik kesimpulan bahwa website Sipapeda dapat ditingkatkan keamanannya menggunakan *algoritma bcrypt*, serta keamanan pada proses login membutuhkan verifikasi *on time password*. Pada penelitian ini hanya menggunakan *algoritma bcrypt* sebagai keamanan data, maka perlu menambahakan beberapa *algoritma* sebagai pembanding untuk lebih meningatkan kemaanan suatu data.

Referensi

[1] Batubara, T. P. (2020). *Analisis Kinerja Algoritma Bcrypt untuk Meningkatkan Keamanan Password dari Brute Force*.

[2] Firdaus, R., Kurniawan, D., & Simamora, E. C. (2017, March). *Implementasi Metode Autentikasi One Time Password (OTPA) Berbasis Mobile Token Pada Aplikasi Ujian Online.* In Prosiding Seminar Nasional Sains, MIPA, Informatika dan Aplikasi (Vol. 3,

No.3).

[3] Editya, G. H., & Mulyati, S. (2018). *Aplikasi Mobile One Time Password Menggunakan* Algoritma *MD5 dan SHA1 untuk Meningkatkan Keamanan Website*. SKANIKA, *1*(2), 618-623.

[4] Khairina, D. M. (2016). *Analisis Keamanan Sistem Login.* Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer, *6*(2), 64-67.

[5] Yunita, N., Komarudin, M., & Brawijaya, A. (2020). *Faktor-Faktor Yang Mempengaruhi Kualitas Layanan Website Bank Syariah Terhadap Perolehan Informasi Nasabah (StudiBni Syariah Kota Bogor).* Banque Syar'i: Jurnal Ilmiah Perbankan Syariah, *6*(1), 01-30.

[6] Naufal, M., & Purwanto, P. (2018). Implementasi Keamanan *Login* Dengan Metode *One Time Password (OTP)* Menggunakan Fungsi *Hash* Algoritma *Sha-512* Pada Smp Negeri 3 Tangerang Selatan. Skanika, 1(1), 335-339.

[7] Qashlim, A. (2016). I*mplementasi Algoritma MD5 Untuk Keamanan Dokumen*. JurnalIlmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar, *2*(2), 10- 15.

[8] Musliyana, Z., Arif, T. Y., Munadi, R., & Sarjana, P. (2016). *Peningkatan sistem keamanan autentikasi single sign on (sso) menggunakan algoritma aes dan one-time password studi kasus: sso universitas ubudiyah indonesia*. Jurnal Rekayasa Elektrika Vol, 12(1).

[9] Simanullang, H. G., & Silalahi, A. P. (2018). Algoritma Blowfish Untuk Meningkatkan Keamanan database Mysql. *Jurnal METHODIKA*, *4*(1), 10-14.

[10] Akbar, M. D., & Antoni, A. (2022). *Aplikasi Absensi Pegawai pada Dinas Komunikasi dan* Informatika *Kabupaten Deli Serdang dengan QR Code Menggunakan Algoritma Bcrypt*. sudo Jurnal Teknik Informatika, *1*(1), 8-16.