INFOKOM : Jurnal Informasi dan Komputer
p-ISSN: 1978-6433
e-ISSN: xxxx-xxxx
Vol.17, No.1, Februari 2024, pp. 51 – 56

IMPLEMENTASI DUA FACTOR AUTHENTICATION DAN MONITORING TRANSACTION PADA APLIKASI PEMESANAN JASA FOTOGRAFI DAN VIDEOGRAFI DI PRIMAPICTURES

Primarazaq Noorshalih P. H*[1], Rizky Septiana A. R [2], Ikhsan Nurul R [3], Irawan Afrianto [4]
[1,2,3,4]*Program Studi Teknik Informatika, Fakultas Teknik, Universitas Komputer Indonesia*
*e-mail: **[1]primarazaq34@gmail.com

Abstrak

Pertumbuhan teknologi informasi yang terus berlanjut telah membawa dampak positif dan tantangan baru bagi pengelola sistem. Universalitas akses dan kemudahan dalam teknologi ini telah membuka peluang bagi penyalahgunaan oleh pihak yang berniat jahat. Keamanan dalam platform website, sebagai pilar utama dalam teknologi informasi, menjadi isu yang semakin penting. Penelitian ini mengusulkan penggunaan mekanisme keamanan tambahan dalam bentuk otentikasi dua faktor (2FA) untuk meningkatkan tingkat keamanan dalam transaksi elektronik (E-Payment). Kami mengimplementasikan sistem ini pada UMKM Primapictures yang bergerak dalam layanan fotografi dan videografi. Metode analisis deskriptif digunakan untuk menggambarkan fakta dan informasi terkait. Hasil pengujian menunjukkan bahwa penggunaan 2FA dan mekanisme pemantauan pemesanan telah berhasil diterapkan dengan baik dalam sistem. Implementasi 2FA mengurangi risiko serangan phishing dan peningkatan keamanan dalam akses masuk. Mekanisme pemantauan juga memberikan respons yang cepat terhadap perilaku mencurigakan. Kesimpulan dan saran yang dihasilkan dari penelitian ini memberikan panduan bagi pengembangan lebih lanjut dalam mengamankan transaksi online.

Kata kunci: Two Factor Authentication (2FA), keamanan transaksi, E-Payment, monitoring pemesanan, pengelolaan keamanan, Primapictures

1. PENDAHULUAN

Kemajuan teknologi informasi yang terus berlanjut memunculkan kekhawatiran bagi pengelola sistem, karena akses yang semakin mudah dan universal membuat mereka rentan terhadap penyalahgunaan oleh pihak-pihak yang berniat jahat[1]. Website adalah wadah yang mengadopsi metode otentikasi yang lebih kuat untuk meningkatkan keamanan serta menjadi pilar utama dalam teknologi informasi. Kemampuannya untuk diakses secara universal, kapan pun dan di mana pun, membawa dampak positif dalam hal keterpaparan risiko kejahatan siber terhadap website tersebut[2]. Perlindungan terus-menerus pada website merupakan langkah penting untuk meningkatkan keamanan situs. Adanya kebutuhan akan mekanisme pengamanan secara real-time menjadi sangat krusial untuk mengurangi risiko serangan yang mungkin terjadi [3]. Sebagian besar situs web mengandalkan metode otentikasi tunggal untuk melindungi akses ke halaman-halaman khusus. Proses otentikasi ini berperan penting dalam membuktikan kebenaran, keaslian, dan validitas data kunci yang dimasukkan untuk masuk ke dalam sistem[4]. Pada implementasinya, otentikasi tunggal masih mengandung kekurangan, dan salah satu kekurangan utamanya adalah rentan terhadap serangan phishing. Menurut Sharma (2022), serangan phishing mampu memperoleh informasi yang digunakan untuk akses sistem, kemudian melancarkan serangan lebih lanjut dengan memanfaatkan data sensitif (seperti username dan password) yang berhasil diperoleh[5]. Oleh karena itu, diperlukan mekanisme keamanan tambahan guna meningkatkan tingkat keamanan pada situs web. Salah satu cara untuk meningkatkan keamanan sistem dapat dilakukan dengan menggunakan teknik kriptografi pada sistem. Teknik kriptografi merupakan salah satu alternatif solusi yang dapat digunakan dalam pengamanan informasi,
beberapa penelitian ,menunjukkan peran dan pentingnya mengamankan data menggunakan kriptografi [6]. Selain itu, para ahli sebelumnya telah mengembangkan berbagai metode keamanan untuk situs web,

History of Article :
Received: Januari, 2024 : Accepted: Januari, 2024

salah satunya adalah two-factor authentication (2FA), yakni metode otentikasi yang melibatkan dua atau lebih langkah otentikasi untuk meningkatkan keamanan dan mengurangi risiko serangan peretasan akun [7]. Otentikasi atau yang juga dikenal sebagai validasi merupakan proses untuk memverifikasi keaslian identitas guna mendapatkan akses ke dalam suatu sistem[8]. Sejumlah penelitian seputar two-factor authentication (2FA) telah dilakukan. Fitriyansyah dan Hazri (2020, 8) mengembangkan OTP (one-time password) dengan menggunakkan SMS (short message service) sebagai bentuk otentikasi ganda, meskipun memiliki kelemahan jika nomor ponsel pengguna disalahgunakan, yang membuat proses OTP menjadi kurang efektif[9]. Selain itu, Mahardhika dan David (2020, 361) berhasil menciptakan mekanisme 2FA menggunakan OTP yang dikirim melalui layanan SMS dan menjelaskan bahwa pengiriman kode OTP melalui SMS memerlukan biaya pulsa, sehingga diperlukan sebuah proses OTP yang bisa memanfaatkan layanan gratis seperti WhatsApp, Telegram, atau e-mail[10].

Primapictures merupakan salah satu UMKM di Kota Bandung yang bergerak dalam menyediakan jasa fotografi dan videografi untuk keperluan acara seperti Wedding, Prewedding, Gathering, dan berbagai acara lainnya yang membutuhkan dokumentasi kegiatan berupa foto dan video dalam kegiatannya. Di Primapictures terhitung pada tahun 2022 rata-rata penjualannya sebanyak 42 penjualan dengan rata-rata per bulannya 3 sampai dengan 4 penjualan. Dari setiap penjualannya rata-rata pendapatan dari tiap transaksi adalah sebesar Rp.1.392.262 dengan jumlah pendapatan total sebesar Rp.58.475.000 di tahun 2022. Dengan besarnya penjualan dari tiap transaksi, maka dibutuhkan jaminan keamanan dalam setiap transaksinya. Maka dari itu pada penelitian ini akan menambahkan keamanan pada saat proses bertransaksi secara elektronik (E-Payment) dengan Midtrans sebagai payment gateway. Payment gateway merupakan system pembayaran online yang berfungsi untuk menggambarkan dan mengautentikasi informasi dalam sebuah transaksi sesuai dengan kebijakan yang telah ditetapkan oleh penyedia layanan[11],[12]. Dalam era online saat ini, payment gateway sangat diminati dan populer, terutama di kalangan pelaku e-commerce. Payment gateway memberikan sejumlah keuntungan dan kemudahan kepada pelaku e-commerce dalam melakukan transaksi keuangan secara digital yang didukung oleh jaringan internet.

Dalam penelitian ini, dirancang dan dibangun suatu sistem yang bertujuan untuk mengatasi masalah yang telah disebutkan sebelumnya[11]. Pendekatan yang diambil adalah dengan menggunakan API Midtrans sebagai Payment Gateway. API pada dasarnya adalah antarmuka yang menghubungkan satu aplikasi dengan aplikasi lainnya. Dengan kata lain, peran utama API adalah menjadi perantara antara berbagai aplikasi yang berbeda, baik dalam satu platform yang sama maupun lintas platform. Midtrans adalah salah satu payment gateway yang membantu memenuhi kebutuhan para pelaku bisnis online dengan menyediakan layanan beragam metode pembayaran seperti transfer bank, dompet elektronik, dan lainnya. Saat ini, sektor e-payment di Indonesia telah mengalami pertumbuhan pesat, dengan banyak perusahaan penyedia layanan e-payment yang turut berkontribusi dalam persaingan pasar[13]. Beberapa bank juga telah berkolaborasi dengan para pengembang untuk menciptakan produk baru yang mendukung perkembangan industri ini. Bahkan, beberapa perusahaan telah mendirikan anak perusahaan untuk bersaing dalam model bisnis baru di sektor e-payment. Di Indonesia, beberapa produk e-payment yang populer antara lain Go-Pay, OVO, ShopeePay, DANA, Kredivo, dan lain sebagainya. Dengan berbagai fakta yang ada, potensi pertumbuhan e-payment di Indonesia sangat besar. Pemerintah melalui Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK) telah mengawasi industri ini. Namun, meskipun demikian, adopsi layanan ini masih terbatas di Indonesia. Terutama, Usaha Mikro, Kecil, dan Menengah (UMKM) yang merupakan 98% dari jumlah pengusaha, belum sepenuhnya mendapatkan layanan finansial. Padahal, di tingkat global, layanan finansial berbasis teknologi yang sedang berkembang dianggap sebagai alternatif terhadap layanan konvensional yang pernah menghadapi masalah dan skandal selama krisis ekonomi pada tahun 2008.

2. METODE PENELITIAN

Metodologi analisis deskriptif merupakan metode yang menggambarkan setiap fakta dan informasi dalam situasi dan kondisi atau peristiwa secara sistematis, faktual dan akurat[14]. Metode ini digunakan dalam penelitian awal dengan tujuan untuk mengumpulkan data dan fakta mengenai kondisi yang terjadi saat ini sebagai bahan referensi untuk mengetahui kondisi pihak pengguna serta faktor pendukung dan penghambat dalam proses pengembangan dan penggunaan dari produk yang dihasilkan. Penelitian ini akan dilakukan melalui serangkaian langkah sebagai berikut:

a) Melakukan Studi Literatur dari sumber-sumber yang berhubungan dengan penelitian

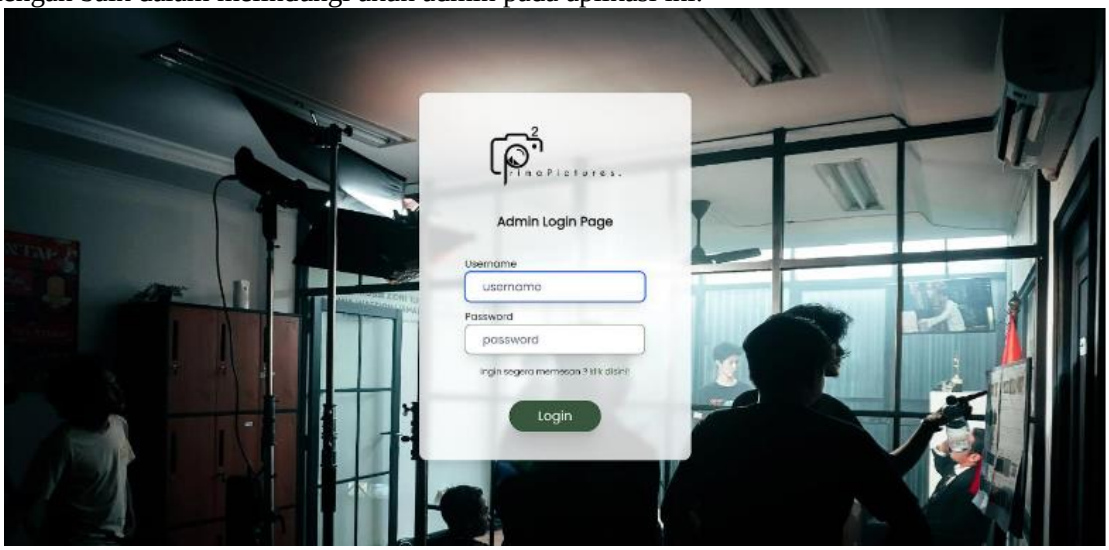
b) Perancangan yang dilakukan menggunakan metode perancangan waterfall
c) Implementasi yang dilakukan adalah dengan menerapkan metode tersebut pada aplikasi yang dikembangkan
d) Pengujian yang dilakukan adalah dengan menguji 2FA dan memonitoring pemesanan pada
web PrimaPictures

3. HASIL DAN PEMBAHASAN

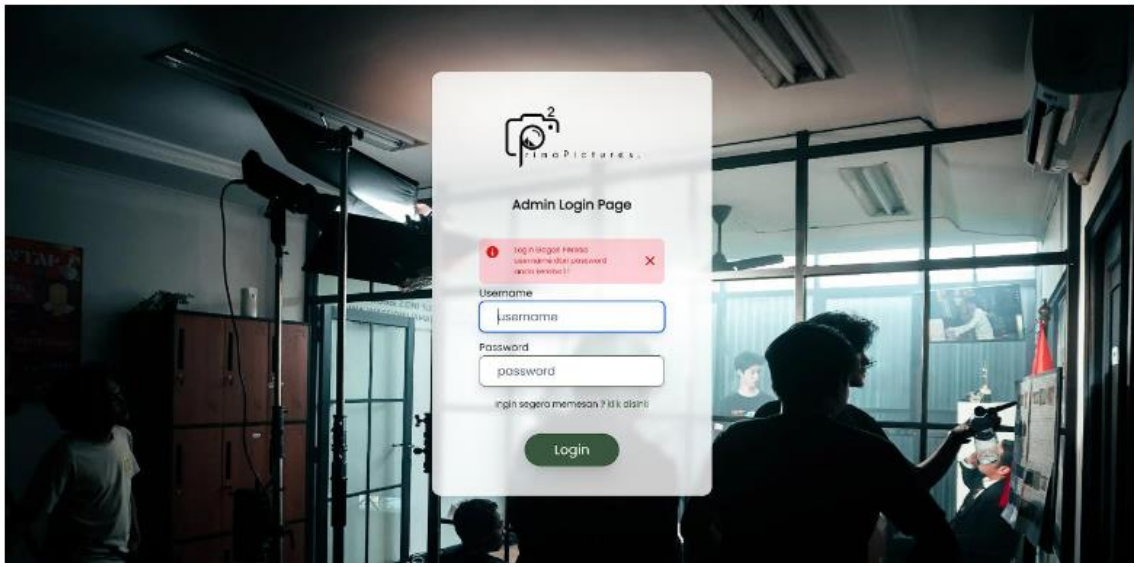
Pengujian sistem merupakan tahapan yang dilakukan menguji fungsionalitas sistem yang sedang diteliti[15]. Hal ini penting dilakukan untuk menemukan celah kesalahan atau kekurangan pada keamanan sistem yang sudah ditambahkan. Selain itu, pengujian dilakukan untuk memastikan bahwa keamanan sistem yang telah ditambahkan sudah memenuhi kriteria yang sesuai dengan tujuan perancangan perangkat lunak. Maka hasil yang didapat dari pengujian implementasikan 2FA dan memonitoring pesanan pada web PrimaPictures sebagai berikut:

3.1 Pengujian Pada Form Login Admin

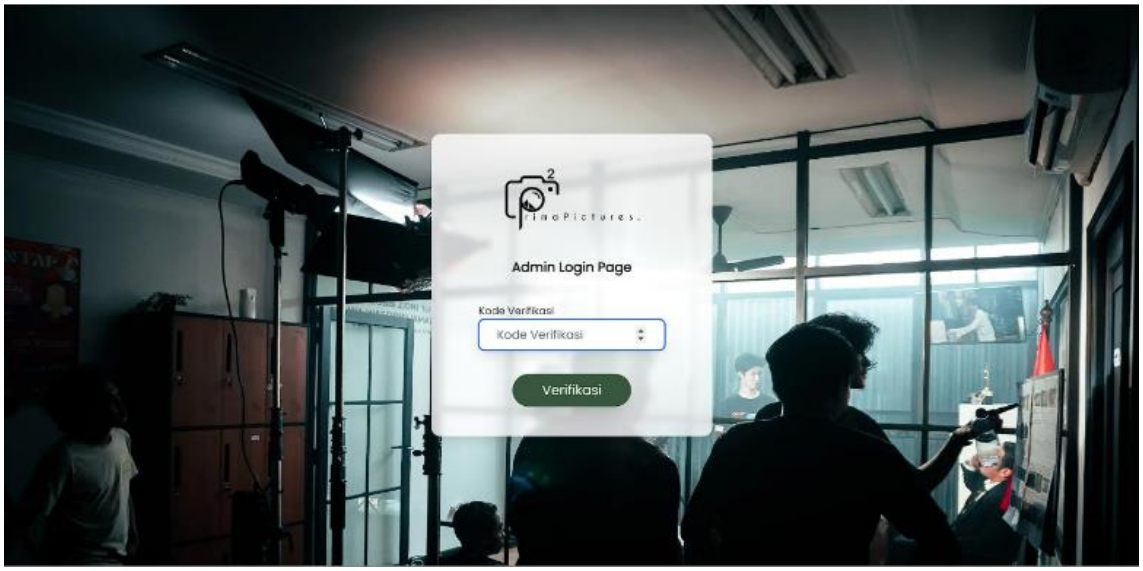
Pada gambar Gambar 1, Anda dapat melihat tampilan halaman login aplikasi. Pada tahap ini, admin diminta untuk memasukkan kredensial mereka, seperti username dan password. Namun, gambar Gambar 2 menunjukkan tampilan yang muncul Ketika pengguna memberikan kredensial yang salah. Sistem memberikan respons bahwa kombinasi username dan password yang dimasukkan tidak valid, dan pengguna diminta untuk memeriksa kembali informasi yang mereka masukkan. Saat admin berhasil memasuki akunnya dengan benar, inilah saat gambar Gambar 3 muncul. Halaman verifikasi akun dengan 2FA muncul di mana admin harus memasukkan kode verifikasi yang dikirimkan melalui metode otentikasi kedua, misalnya aplikasi otentikator atau pesan teks. Jika kode verifikasi cocok, admin berhasil mengakses halaman berikutnya dalam aplikasi PrimaPictures. Dengan melakukan serangkaian pengujian seperti ini, kami memastikan bahwa langkah-langkah keamanan, termasuk 2FA, berfungsi dengan baik dalam melindungi akun admin pada aplikasi ini.



Gambar 1. Halaman login admin



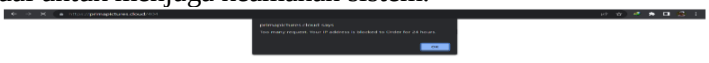
Gambar 2. Kesalahan memasukkan username atau password



Gambar 3. Verifikasi akun admin menggunakan two factor authentication

3.2 Pengujian memonitoring pemesanan

Gambar 4 mengindikasikan bahwa alamat IP telah diblokir oleh situs web ini. Penyebabnya adalah karena tindakan yang tidak biasa, sebagai contoh kami melakukan refresh halaman konfirmasi pembayaran secara berulang sekitar 10 kali. Gambar ini memberikan pesan jelas bahwa tindakan tersebut dianggap tidak wajar oleh sistem, sehingga IP diblokir sebagai langkah keamanan. Melalui pengujian ini, kami dapat mengamati dan mengidentifikasi bagaimana platform PrimaPictures merespons perilaku yang mencurigakan dan mengambil tindakan yang sesuai untuk menjaga keamanan sistem.



Gambar 4. Pemblokiran IP oleh web primapictures

4. KESIMPULAN

Berdasarkan dari hasil penelitian yang telah dilakukan, diperoleh beberapa kesimpulan, diantaranya adalah dari aplikasi yang sudah ada dilakukan penambahan fitur Two Factor Authentication dan monitoring pemesanan dalam upaya meningkatkan keamanan sistem berhasil dilakukan, implementasi Two Factor Authentication pada aplikasi telah dilakukan dan dapat berfungsi sesuai dengan kebutuhan fungsionalnya, penggunaan Two Factor Authentication meningkatkan keamanan sistem khususnya pada login admin, implementasi monitoring pemesanan pada aplikasi telah dilakukan dan dapat berfungsi sesuai dengan kebutuhan fungsionalnya, penggunaan monitoring pemesanan membatasi pengguna untuk melakukan pemesanan dalam 24 jam. Adapun yang lainnya adalah hal-hal yang diperlukan guna meningkatkan pengembangan penelitian ini dengan menerapkan JWT (JSON Web Tokens) untuk menjaga status autentikasi dan membantu dalam manajemen token autentikasi dan mengurangi kebutuhan untuk mengingat sesi dalam server, mengembangkan Mobile App dengan memberikan fleksibilitas lebih besar bagi pelanggan dalam mengakses dan memesan layanan Primapictures.

DAFTAR PUSTAKA

[1] Y. Fitriyansyah and M. Hazri, "Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password," SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI, vol. XXX, no. 1, pp. 1-14, 2020.

[2] H. R. Herdiantoro and M. R. R. Islami, "IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) DAN FIREWALL POLICIES DALAM MENGAMANKAN WEBSITE," JMIK (JURNAL MAHASISWA ILMU KOMPUTER), vol. IV, no. 1, pp. 1-9, 2023.

[3] M. Z. Huwaidi and S. Destya, "Mencegah Serangan Rekayasa Sosial dengan Human Firewall," JUSTIN (Jurnal Sistem dan Teknologi Informasi), vol. x, no. 1, pp. 107-1121, 2022.

[4] D. Kurniawan, E. Zusrony and R. A. Kusumajaya, "ANALISA PERSEPSI PENGGUNA LAYANAN PAYMENT GATEWAY PADA FINANCIAL TECHNOLOGY DENGAN METODE EUCS," Jurnal INFORMA Politeknik Indonesia Surakarta , vol. IV, no. 3, pp. 1-5, 2018.

[5] G. C. Mahardhika and F. David, "Implementasi Two Factor Authentication (2FA) pada Sistem Keamanan Otentikasi User di Aplikasi Kasir Legends Barbershop," USTIN (Jurnal Sistem dan Teknologi Informasi), vol. VIII, no. 4, pp. 357-361, 2020.

[6] N. Taliasih and I. Afrianto, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," Jurnal Nasional Teknologi dan Sistem Informasi, vol. VI, no. 1, pp. 9-18 , 2020.

[7] C. Mustaqim, "IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN ALGORITMA RSA SEBAGAI METODE OTENTIKASI LOGIN PADA SI-ABKA (SISTEM AMAL BAKTI KEMENTRIAN AGAMA)," pp. 1-60, 2020.

[8] S. D. Risqiwati and E. A. Irawan, "Realtime Pencegahan Serangan Brute Force dan DDOS Pada Ubuntu Server," Techno.COM, vol. XVII, no. 4, pp. 347-354, 2018.

[9] L. Namira, "Faktor-Faktor Yang Mempengaruhi Niat UMKM di Kota PadangMenggunakan e-Payment sebagai Metode Pembayaran," Owner: Riset & Jurnal Akuntansi,vol. VI, no. 1, pp. 212-224, 2022.

[10] V. H. ranatawijaya and H. Yulianto, "Penerapan API (Application Programming Interface)MIDTRANS Sebagai Payment Gateway Pada Indekos Berbasis Website," JOINTECOMS
(Journal of Information Technology and Computer Science) , vol. II, no. 4, pp. 254-262,2022

[11] I. P. Saputra , "APLIKASI BERBASIS WEB GUNA MEMONITORING KE AKTIFAN IP PUBLIC," BULLETIN OF NETWORK ENGINEER AND INFORMATICS, vol. I, no. 2, pp. 1-6, 2023.

[12] H. Setiawan, D. Sartika and B. G. Ramadhan, "IMPLEMENTASI TIME-BASED ONE TIME PASSWORD (TOTP) PADA SISTEM TWO FACTOR AUTHENTICATION (2FA)," Jurnal Teknologi, vol. XIII, no. 1, pp. 63-68, 2020.

[13] P. Sharma, M. F. Ansari and B. Dash, "Anti-Phishing Techniques -A Review of Cyber Defense Mechanisms," International Journal of Advanced Research in Computer and Communication Engineering , vol. XI, no. 7, pp. 153-160, 2022.

[14] Afrianto and A. Setiyadi, "Sistem Informasi Monitoring Perdagangan, Pariwisata Dan Investasi Indonesia Dengan Negara-Negara Di Kawasan Amerika Dan Eropa," INFORMATICS FOR EDUCATORS AND PROFESSIONALS, vol. III, no. 2, pp. 171-184, 2019.

[15] I. Afrianto, S. atin and T. R. D. Suseno, "PEMODELAN SISTEM PENCATATAN DATA AKADEMIK SEKOLAH BERBASIS TEKNOLOGI BLOCKCHAIN," ResearchGate, Bandung, 2023.