Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi Curva Elliptic

JALUR SCIENTIST

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

Disusun oleh

Nevy Bella Samantha

19.83.0373

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

PERANCANGAN KEAMANAN PENGGUNA CARDLESS DARI ANCAMAN CYBER CRIME MENGGUNAKAN KRIPTOGRAFI CURVA ELLIPTIC

JALUR SCIENTIST

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

Disusun oleh

Nevy Bella Samantha

19.83.0373

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

NASKAH PUBLIKASI

PERANCANGAN KEAMANAN PENGGUNA CARDLESS DARI ANCAMAN CYBER CRIME MENGGUNAKAN KRIPTOGRAFI CURVA ELLIPTIC

yang disusun dan diajukan oleh

Nevy Bella Samantha

19.83.0373

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 November 2023

Dosen Pembimbing,

Senie Destya, M.Kom
NIK. 190302312

HALAMAN PENGESAHAN

SKRIPSI

PERANCANGAN KEAMANAN PENGGUNA CARDLESS DARI ANCAMAN CYBER CRIME MENGGUNAKAN KRIPTOGRAFI CURVA ELLIPTIC

yang disusun dan diajukan oleh

Nevy Bella Samantha

19.83.0373

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 November 2023

Susunan Dewan Penguji

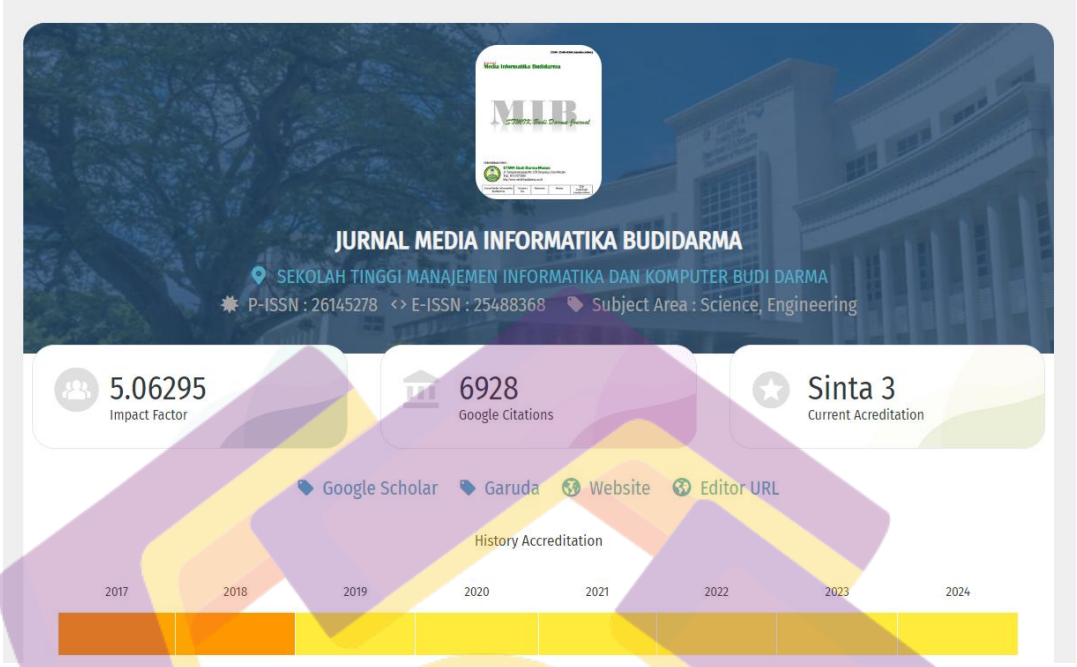
Nama Penguji	Tanda Tangan
Banu Santoso, S.T., M.Eng **NIK. 190302327**	
Muhammad Koprawi, S.Kom., M.Eng **NIK. 190302454**	
Senie Destya, M.Kom **NIK. 190302312**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 November 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom.
NIK. 190302096

IDENTITAS JURNAL



Tentang Jurnal

ISSN (Online)	:	2548-8368
Issues	:	4 kali/tahun (Januari, April, Juli, Oktober)
Index	:	Google Scholar, Garuda, dan SINTA 3, IPI, OneSearch, MORAREF, Dimensions, Crossref, Scilit, PKP INDEX, OpenAIRE EXPLORE, BASE, ROAD
DOI Prefix	:	hhtps://doi.org/10.30865/mib.v7i3.6100

LEMBAR REVIEW

Surya Darma Nasution, M.Kom <suryadarma@stmik-budidarma.ac.id>
to me, Senie

Indonesian > English Translate message

Bella Nevy Bella Samantha:

We have reached a decision regarding your submission to JURNAL MEDIA INFORMATIKA BUDIDARMA, "Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi Curva Elliptic".

Our decision is: Revisions Required

Surya Darma Nasution, M.Kom
(SCOPUS ID: 57202607800, Universitas Budi Darma, Medan)
Phone -
suryadarma@stmik-budidarma.ac.id

Reviewer A:

1. Kontribusi artikel terhadap pengembangan ilmu pengetahuan:
   Memiliki Kontribusi

2. Penulisan Judul Artikel (CEK dan Komentari: Pada judul memiliki masalah yang di bahas, metode/solusi penyelesaian masalah, dan informatif. Judul memiliki kata sebanyak 14-18 kata):
   Pada judul gambaran metode sudah terlihat

3. Penulisan Abstrak (CEK dan Komentari: Pada Abstrak harus memiliki masalah

3. Penulisan Abstrak (CEK dan Komentari: Pada Abstrak harus memiliki masalah yang di bahas pada penelitian, solusi/metode yang digunakan, tujuan dan kontribusi dari penelitian, serta hasil sementara yang dicapai. Hasil bisa berupa angka/persentase/linguistik):
   Hasil dari penelitian belum di gambarkan di abstrak.

4. Isi PENDAHULUAN (CEK dan Komentari: Isi pendahuluan menggambarkan masalah penelitian, metode pembanding, penelitian sejenis/terkait, GAP/Perbedaan dari penelitian sebelumnya, tujuan penelitian yang akan dilakukan, mengkaitkan teori yang digunakan dengan RUJUKAN/REFERENSI/KUTIPAN yang terdapat pada DAFTAR PUSTAKA, serta memiliki pernyataan kontribusi dari hasil penelitian. Referensi/kutipan ditulis dengan format IEEE yang menggunakan Soft Referensi Ilmiah mis. Mendeley).:
   Penelitian terdahulu, atau penelitian terkait belum ada, harap ditambahkan.

5. Penulisan METODOLOGI PENELITIAN (CEK dan Komentari: Bagian metodologi ini harus memiliki tahapan penelitian yang menggambarkan tahapan apa yang dilakukan pada penelitian, terlihat penerapan solusi/metode pada tahapan penelitian, serta memiliki kajian pustaka dari algoritma/metode yang digunakan. Setiap penulisan WAJIB memiliki referensi/kutipan dengan format IEEE yang ditulis menggunakan Soft Referensi Ilmiah mis. Mendeley):
   Tahapan penelitian sudah dijabarkan pada metodologi penelitian. Uraian dari metode yang di gunakan sudah ada.

6. Penulisan HASIL dan PEMBAHASAN (CEK dan Komentari: Bagian ini menguraikan tahapan dari penerapan algoritma/metode dalam menyelesaikan masalah, serta hasil yang di peroleh dari algoritma/metode yang digunakan. Hasil pengujian algoritma/metode. Pembahasan dapat juga membandingkan hasil penelitian dengan penelitian sejenis. Bila penelitian berbentuk pembuatan alat, di

LEMBARAN PERSETUJUAN (LoA)

JURNAL MEDIA INFORMATIKA BUDIDARMA
eISSN 2548-8368 / pISSN 2614-5278
Sekretariat : UNIVERSITAS BUDI DARMA | Jl. Sisingamangaraja No. 338, Medan, Sumatera Utara
Website: https://ejurnal.stmik-budidarma.ac.id/index.php/mib
Email: mib.stmikbd@gmail.com

Medan, 8 Oktober 2023

No : 871/MIB/LOA/X/2023
Lamp : -
Hal : Surat Penerimaan Naskah Publikasi Jurnal

KepadaYth,
Bapak/Ibu **Nevy Bella Samantha**
Di Tempat

Terimakasih telah mengirimkan artikel ilmiah untuk diterbitkan pada **Jurnal Media Informatika Budidarma** (eISSN 2548-8368 / pISSN 2614-5278), dengan judul:

Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi Curva Elliptic

Penulis: **Nevy Bella Samantha, Senie Destya, Wahid Miftahul Ashari(*)**

Berdasarkan hasil review dari reviewer, artikel tersebut dinyatakan DITERIMA untuk dipublikasikan pada **Volume 7, Nomor 4, Oktober 2023**.

Sebagai informasi QR-Code digunakan untuk melihat link LOA Jurnal Media Informatika Budidarma, **Volume 7, Nomor 4, Oktober 2023** yang telah dikeluarkan. Mohon segera untuk mengirimkan Copyright Transfer Form ke Email Jurnal MIB.

Demikian informasi yang kami sampaikan, atas perhatiannya kami ucapkan terimakasih.

Hormat Kami,

Surya Darma Nasution, M.Kom
Ketua Editor Jurnal MIB

Tembusan:
1. Author
2. Files

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor 4, Oktober 2023, Page 1706-1715
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI: 10.30865/mib.v7i4.6827

Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi Curva Elliptic

Nevy Bella Samantha, Senie Destya, Wahid Miftahul Ashari*

Fakultas Ilmu Komputer, Program Studi Ilmu Komputer, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia
Email: [1]nevy.2000@students.amikomac.id, [2]seniedestya@amikom.ac.id, [3,*]wahidashari@amikom.ac.id
Email Penulis Korespondensi: wahidashari@amikom.ac.id

Abstrak−Pada era ini teknologi telah menemukan inovasi baru dengan menciptakan cara-cara praktis dalam bertransaksi. Transaksi tarik tunai saat ini jauh lebih mudah karena telah ditemukan cara baru yaitu masyarakat dapat bertransaksi tanpa menggunakan kartu. Hal ini tentu sangat berguna bagi orang-orang yang dompetnya sering tertinggal. Kemudahan dalam melakukan transaksi ini disebut Cardless. Cardless sendiri merupakan layanan tarik tunai tanpa kartu yang menawarkan proses transaksi cepat dan hemat waktu. Selain itu, kartu tanpa kartu juga memiliki beberapa keunggulan, diantaranya kartu ATM lebih aman dari risiko tertelan atau tertinggal ATM, serta terhindar dari risiko penipuan. Selayaknya teknologi pada umumnya yang diciptakan oleh manusia cardless tentunya juga memiliki kekurangan. Transaksi ini berpotensi pencurian identitas, pengeluaran yang tidak terkendali, kompromi sistem, dan tidak semua orang menggunakan transaksi tarik tunai tanpa kartu ini karena kurangnya sosialisasi penggunaan transaksi cardless. Pada penelitian ini peneliti ingin merekomendasi perancangan keamanan tambahan pada aplikasi m-banking, berbeda dari penelitian terdahulu kali ini peneliti menggunakan metode Curva Elliptic. Yang menjadi subyek dari penilitian ini adalah para pengguna cardless. Adapun tujuan yang ingin dicapai pada penelitian ini adalah keamanan dari aplikasi m-banking saat menggunakan transaksi cardless menjadi lebih aman dikarenakan telah ditambahkan perhitungan dari algoritma untuk mengacak atau enkripsi PIN, fungsi dari dienkripsinya PIN sendiri bertujuan untuk membuat semakin sulit pelaku kejahatan berhasil menjalankan tindak kejahatan. Apabila tidak menambahkan tingkat keamanan seperti yang direkomendasikan oleh penulis makan pihak bank harus memikirkan cara lain untuk meningkatkan keamanan saat melakukan transaksi cardless karena selanjutnya akan semakin banyak nasabah atau pengguna yang menjadi korban. Dari hasil enkripsi pada penelitian ini PIN yang tadinya 312143 setelah dilakukan proses enkripsi maka PIN tersebut berubah menjadi DUDSDTDSDVDU. Tentunya ke depan teknologi akan semakin berkembang dan mungkin akan tercipta cela yang lebih besar, namun hingga saat ini kriptografi Curva Elliptic masih menjadi kriptografi yang sulit untuk dipecahkan. Dengan begitu sedikit kemungkinan para pelaku cybercrime bisa membobol.

Kata Kunci: Cardles; Cyber Crime; Curva Elliptic; Keamanan Data; Kriptografi

Abstract−In this era, technology has discovered new innovations by creating practical ways of making transactions. Cash withdrawal transactions are now much easier because a new way has been discovered, where people can make transactions without using a card. This is certainly very useful for people whose wallets are often left behind. This ease of carrying out transactions is called Cardless. Cardless itself is a cardless cash withdrawal service that offers a fast and time-saving transaction process. Apart from that, cardless cards also have several advantages, including ATM cards being safer from the risk of being swallowed or left behind by the ATM, and avoiding the risk of fraud. Like technology in general created by humans, cardless certainly also has disadvantages. This transaction has the potential for identity theft, uncontrolled spending, system compromise, and not everyone uses cardless cash withdrawal transactions due to lack of socialization of the use of cardless transactions. In this research, the researcher wants to recommend designing additional security in the m-banking application. Different from previous research, this time the researcher used the Elliptic Curve method. The subjects of this research are cardless users. The goal to be achieved in this research is that the security of the m-banking application when using cardless transactions becomes safer because the calculation of the algorithm has been added to randomize or encrypt the PIN. The function of encrypting the PIN itself is aimed at making it more difficult for criminals to successfully carry out crimes. . If the level of security is not added as recommended by the author, the bank will have to think of other ways to increase security when carrying out cardless transactions because then more customers or users will become victims. From the encryption results in this research, the PIN was previously 312143, after the encryption process was carried out, the PIN changed to DUDSDTDSDVDU. Of course, in the future technology will continue to develop and perhaps even bigger flaws will be created, but up to now Elliptic Curve cryptography is still cryptography that is difficult to solve. With so little chance that cybercrime perpetrators can break in.

Keywords: Cardless; Cyber Crime; Curva Elliptic; Data security; Cryptography

1. PENDAHULUAN

Perkembangan teknologi semakin hari semakin maju, sehingga memudahkan masyarakat untuk melakukan tarik tunai tanpa harus antre di bank. ATM atau yang biasa kita sebut dengan ATM merupakan suatu kemudahan yang ditemukan untuk membantu proses transaksi dengan cara menghemat waktu masyarakat.Pengamanan ATM berupa nomor PIN (Personal Identification Number) yang dimiliki nasabah.Namun,dibalik kemudahan ATM tersebut juga terdapat beberapa kekurangan antara lain kartu ATM mudah rusak, kartu ATM tertelan mesin, nomor PIN dicuri, kartu ATM terblokir akibat salah memasukkan PIN sebanyak 3 kali.

Bersumber dari Kompas.com, pada Januari 2022, Bank Indonesia (BI) melihat pertumbuhan pesat transaksi keuangan digital. Hal ini sejalan dengan meningkatnya ekspektasi dan preferensi masyarakat terhadap belanja online,menjamur dan nyamannya sistem pembayaran digital, serta akselerasi perbankan digital. Menurut Ronald M Hutabarata 2010[1]. Mobile banking atau yang biasa kita sebut dengan M-Banking merupakan inovasi yang dikembangkan oleh bank melalui handphone sebagai alat komunikasi dengan perangkat yang hampir mirip dengan ATM kecuali untuk penarikan tunai. Pada era ini teknologi telah menemukan inovasi baru dengan menciptakan

Submitted: **24/09/2023**; Accepted: **18/10/2023**; Published: **22/10/2023**