

Verifikasi Logika Autentikasi Sistem Login Menggunakan Penggunaan Tabel Kebenaran

Mila Nur Alwiyyah¹, Qisti Auliya²

^{1,2} Teknik Informatika, Sekolah Tinggi Teknologi Indonesia, Cirebon, Jawa Barat, Indonesia
Email: milanuralwiyyah658@gmail.com

Abstract—Authentication is a fundamental component of login systems to ensure that only legitimate users are granted access to digital services. In practice, authentication mechanisms are often implemented directly in program code without a clear examination of the formal logical structure underlying the decision-making process. This paper adopts propositional logic to model and verify a basic login authentication mechanism using truth tables. The login process is represented as a set of logical propositions describing the validity of a username and a password, which are then systematically evaluated to analyze logical consistency and potential error scenarios. The results show that truth tables clearly identify all possible combinations of input conditions that lead to successful or failed authentication and help detect logical flaws such as false positives. In addition, a simple C++-based authentication simulation is presented to demonstrate how the logical structure $A \wedge B$ (valid username $\wedge$ valid password) can be directly mapped into program code. The analysis confirms that truth tables provide a strong mathematical framework for validating authentication logic and improving the reliability and security of login systems.

Keywords— authentication, truth table, propositional logic, system verification, login security.

Abstrak — Autentikasi merupakan komponen fundamental dalam sistem login untuk memastikan bahwa hanya pengguna yang valid yang dapat mengakses suatu layanan digital. Namun, proses autentikasi sering dipandang semata-mata sebagai implementasi pemrograman tanpa meninjau dasar logika formal yang menyusunnya. Penelitian ini menggunakan pendekatan Logika Proposisi untuk memodelkan proses autentikasi login dan memverifikasinya melalui tabel kebenaran. Proses login direpresentasikan sebagai rangkaian proposisi yang menggambarkan kondisi validitas username dan password, kemudian dianalisis secara sistematis untuk melihat konsistensi dan kemungkinan terjadinya kesalahan logika. Melalui metode ini, penelitian menunjukkan bahwa tabel kebenaran mampu mengidentifikasi kombinasi kondisi yang menghasilkan autentikasi berhasil maupun gagal secara jelas, sekaligus mendeteksi potensi skenario yang tidak sesuai dengan aturan sistem. Selain itu, penelitian ini menyertakan implementasi simulasi autentikasi menggunakan bahasa pemrograman C++ untuk menunjukkan bagaimana struktur logika $A \wedge B$ (username valid $\wedge$ password valid) diterapkan secara langsung dalam kode program. Simulasi tersebut memperkuat pembuktian bahwa model logika proposisional dapat dipetakan secara konsisten ke proses autentikasi nyata pada sistem login. Hasil analisis menegaskan bahwa penggunaan tabel kebenaran memberikan kerangka matematis yang kuat untuk memvalidasi proses autentikasi sekaligus meningkatkan keandalan dan keamanan sistem login.

Kata Kunci— autentikasi, tabel kebenaran, logika proposisi, verifikasi sistem, keamanan login, simulasi C++.

I. PENDAHULUAN

Autentikasi login merupakan salah satu mekanisme keamanan yang paling umum digunakan dalam sistem informasi modern. Hampir seluruh aplikasi berbasis web maupun mobile mengandalkan proses login untuk membatasi akses pengguna dan mencegah pihak yang tidak berwenang memasuki sistem. Meskipun implementasi autentikasi telah menjadi praktik yang lazim, banyak pengembang hanya berfokus pada aspek pemrograman atau tampilan antarmuka tanpa memahami struktur logika formal yang mendasarinya. Padahal, setiap keputusan autentikasi pada dasarnya merupakan hasil evaluasi kondisi logis antara username dan password yang diberikan oleh pengguna.

Kesenjangan yang muncul adalah kurangnya alat verifikasi matematis untuk memastikan bahwa aturan

autentikasi telah disusun secara konsisten dan bebas dari skenario kesalahan. Kesalahan logika sekecil apa pun memiliki potensi menjadi celah keamanan yang serius. Misalnya, kondisi ketika sistem memberikan akses meskipun hanya salah satu dari username atau password bernilai benar (false positive). Dengan memanfaatkan tabel kebenaran, seluruh kombinasi input autentikasi dapat dianalisis secara menyeluruh sehingga sistem dapat diverifikasi berdasarkan seluruh kemungkinan keadaan yang mungkin terjadi.

Topik ini sangat relevan dalam bidang Teknik Informatika karena menghubungkan konsep logika matematika, khususnya Logika Proposisi, dengan praktik nyata dalam keamanan sistem. Pemodelan logika memberikan pemahaman yang lebih dalam mengenai hubungan antara proses komputasi dan struktur logika yang mengatur keputusan sistem. Selain itu, pendekatan

matematis ini membantu mahasiswa dan pengembang memahami bahwa keamanan tidak hanya bergantung pada kode, tetapi juga pada ketepatan perumusan logika yang mendasarinya.

Dalam penelitian ini, proses autentikasi login dimodelkan sebagai proposisi logis dan diverifikasi menggunakan tabel kebenaran. Selain memberikan analisis formal, penelitian ini juga menyertakan implementasi simulasi login menggunakan bahasa C++ untuk menunjukkan bagaimana model logika $A \wedge B$ (username valid $\wedge$ password valid) diterapkan langsung dalam kode program. Simulasi tersebut memperkuat hubungan antara teori logika dan implementasi praktis dalam sistem autentikasi.

Pembahasan pada penelitian ini difokuskan pada autentikasi dasar berbasis username dan password, tanpa melibatkan faktor keamanan tambahan seperti OTP, biometrik, atau enkripsi data. Pembatasan ini bertujuan untuk memastikan bahwa analisis logika dapat ditinjau secara mendalam dan terfokus pada struktur dasar autentikasi.

Berdasarkan pembatasan tersebut, tujuan dari penulisan penelitian ini adalah untuk menganalisis dan memverifikasi logika autentikasi dasar sistem login berbasis username dan password menggunakan tabel kebenaran, sehingga struktur logika autentikasi dapat ditinjau secara sistematis dan konsisten.

II. TINJAUAN PUSTAKA

Beberapa penelitian sebelumnya telah mengkaji penerapan logika formal dan model matematis dalam bidang keamanan komputer dan verifikasi sistem. Munir [1], [2] membahas logika proposisi dan tabel kebenaran sebagai alat fundamental dalam penalaran ilmu komputer, serta menekankan perannya dalam memvalidasi konsistensi logika pada sistem komputasi. Karya-karya tersebut menjadi landasan teoretis dalam memodelkan proses pengambilan keputusan, termasuk mekanisme autentikasi, ke dalam bentuk proposisi logis.

Penelitian oleh Stallings [6] dan Bishop [8] menegaskan bahwa autentikasi merupakan komponen inti dalam keamanan komputer, di mana kesalahan pada kondisi logika dapat menyebabkan kerentanan serius seperti akses tidak sah. Meskipun fokus utama kajian tersebut adalah prinsip dan praktik keamanan sistem, mekanisme autentikasi yang dibahas secara implisit sangat bergantung pada ketepatan logika dalam alur proses autentikasi.

Silberschatz dkk. [7] mengkaji mekanisme keamanan pada sistem operasi dan menjelaskan bagaimana keputusan autentikasi dan kontrol akses diterapkan pada tingkat sistem. Walaupun pembahasan lebih menitikberatkan pada aspek implementasi, keputusan kontrol akses tersebut pada dasarnya dapat dianalisis secara formal menggunakan logika proposisi dan tabel kebenaran.

Penelitian lain, seperti yang dikemukakan oleh Goguen [5], membahas peran logika secara lebih luas dalam ilmu komputer, termasuk dalam spesifikasi dan verifikasi sistem. Pendekatan ini mendukung gagasan bahwa metode logika formal dapat digunakan untuk memverifikasi

kebenaran perilaku perangkat lunak. Selain itu, sumber daring seperti GeeksforGeeks [3] dan ITBox.id [4] menunjukkan penerapan praktis tabel kebenaran dalam berbagai permasalahan komputasi nyata, sehingga memperkuat relevansi tabel kebenaran baik dalam konteks pendidikan maupun implementasi praktis.

Dibandingkan dengan penelitian-penelitian sebelumnya, penelitian ini secara khusus menitikberatkan pada penggunaan tabel kebenaran sebagai alat verifikasi logika autentikasi dasar pada sistem login. Selain itu, penelitian ini secara eksplisit memetakan model logika proposisional ke dalam implementasi program menggunakan bahasa C++, sehingga menjembatani kesenjangan antara teori logika formal dan praktik pengembangan perangkat lunak dalam konteks keamanan sistem.

A. Logika Proposisi

Logika Proposisi adalah cabang logika formal yang mempelajari hubungan antara pernyataan (proposisi) yang hanya memiliki dua nilai kebenaran, yaitu benar (True) atau salah (False). Dalam konteks sistem login, setiap proses pemeriksaan kredensial dapat dimodelkan sebagai proposisi. Misalnya:

$A = \text{"username valid"}$

$B = \text{"password valid"}$

Proses autentikasi kemudian direpresentasikan sebagai proposisi gabungan $A \wedge B$, yang berarti autentikasi hanya berhasil apabila kedua kondisi bernilai benar. Dengan pendekatan ini, proses login tidak hanya dilihat sebagai kode program, tetapi sebagai struktur logika formal yang dapat diverifikasi secara matematis.

Penggunaan logika proposisi pada autentikasi login memberikan keuntungan berupa pemetaan proses komputasi ke dalam representasi matematis yang lebih terstruktur. Hal ini membantu mendeteksi potensi kesalahan logika yang tidak terlihat hanya melalui pemeriksaan kode.

B. Negasi (NOT)

Negasi digunakan untuk membalikkan nilai suatu proposisi. Jika proposisi p bernilai benar, maka negasinya, $\neg p$ (NOT p), bernilai salah, dan sebaliknya. Dalam autentikasi login, negasi relevan untuk menyatakan kondisi kesalahan, seperti :

$\neg A = \text{"username tidak valid"}$

$\neg B = \text{"password tidak valid"}$

Negasi digunakan untuk memodelkan kasus-kasus gagal autentikasi.

C. Konjungsi (AND)

Konjungsi adalah operator logika yang menghubungkan dua proposisi dengan kata “dan”. Konjungsi hanya bernilai benar ketika kedua proposisi bernilai benar. Tabel kebenarannya adalah :

Tabel 1. Tabel Kebenaran Konjungsi

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

Dalam sistem login, operator konjungsi adalah inti logika autentikasi karena sistem hanya akan memberikan akses jika username dan password keduanya valid. Jika salah satu tidak valid, akses harus ditolak. Logika ini digunakan pula pada implementasi simulasi program C++.

D. Disjungsi (OR)

Disjungsi merupakan operator logika yang bernilai benar jika salah satu atau kedua proposisi bernilai benar. Tabel kebenarannya adalah :

Tabel 2. Tabel Kebenaran Disjungsi

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

Dalam autentikasi login, operator OR tidak umum digunakan untuk keputusan akses karena berpotensi memberikan celah keamanan. Namun, operator ini relevan dalam analisis kasus, seperti validasi input opsional atau aturan fallback pada sistem tertentu.

E. Implikasi (IF-THEN)

Implikasi adalah operator logika yang menyatakan hubungan sebab-akibat antara dua proposisi dan dituliskan sebagai $p \rightarrow q$. Tabel kebenarannya:

Tabel 3. Tabel Logika Implikasi (IF-THEN)

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Pada sistem login, implikasi digunakan untuk merumuskan aturan, seperti :

“Jika username salah, maka akses harus ditolak.”

“Jika password tidak valid, maka sistem tidak memberikan akses.”

Implikasi membantu memformalkan kebijakan autentikasi.

F. Tabel Kebenaran

Tabel kebenaran adalah alat yang digunakan untuk mengevaluasi semua kemungkinan kombinasi nilai kebenaran dari proposisi yang terlibat dalam suatu ekspresi logika. Dalam autentikasi login, tabel kebenaran digunakan untuk :

- Memverifikasi keakuratan aturan autentikasi.
- Mengidentifikasi kondisi yang seharusnya menghasilkan akses atau penolakan.
- Menemukan potensi kesalahan seperti false positive dan false negative.

Dengan tabel kebenaran, sistem dapat diverifikasi secara menyeluruh meskipun implementasinya dalam kode memiliki kompleksitas tertentu.

G. Autentikasi Sistem Login

Autentikasi merupakan proses yang dilakukan untuk memverifikasi identitas pengguna sebelum sistem memberikan akses ke data atau layanan tertentu. Pada sistem login konvensional, autentikasi bergantung pada dua komponen utama :

- Username, sebagai identitas pengguna
- Password, sebagai bukti kepemilikan identitas

Kedua data tersebut harus sesuai dengan informasi yang tersimpan dalam basis data sistem. Jika salah satu tidak cocok, akses akan ditolak. Hal ini sejalan dengan prinsip dasar keamanan informasi, yaitu menjaga :

Kerahasiaan (Confidentiality)

Integritas (Integrity)

Ketersediaan (Availability)

Autentikasi merupakan gerbang utama untuk menjaga kerahasiaan dan integritas, sehingga sangat penting untuk memastikan bahwa logika autentikasi berjalan dengan benar.

Dalam konteks analisis logika, autentikasi sistem login sangat relevan karena prosesnya dapat dipetakan menjadi serangkaian proposisi logis, seperti:

$A = \text{username valid}$

$B = \text{password valid}$

$C = \text{hasil autentikasi}$

Hal ini memungkinkan proses autentikasi untuk dianalisis secara matematis dan diverifikasi menggunakan tabel kebenaran. Dengan memetakan mekanisme autentikasi ke dalam model logika proposisi, pengembang dapat memastikan bahwa keputusan sistem tidak hanya bergantung pada implementasi kode, tetapi juga pada landasan logika yang terstruktur dan formal.

Pendekatan logika ini juga penting saat dikembangkan menjadi implementasi program nyata, seperti simulasi login berbasis C++, karena memungkinkan pengembang untuk memastikan bahwa hasil program selaras dengan model matematis yang telah dibuat.

III. METODOLOGI PENELITIAN

A. Deskripsi Kasus

Studi kasus pada penelitian ini berfokus pada proses autentikasi login yang menggunakan dua input utama, yaitu username dan password. Pada sistem login

konvensional, autentikasi dilakukan dengan mencocokkan input pengguna dengan data yang tersimpan di basis data. Namun, dalam model matematis, proses tersebut disederhanakan menjadi evaluasi dua kondisi logis :

- apakah username valid (A),
- dan apakah password valid (B).

Kedua kondisi inilah yang menentukan apakah autentikasi berhasil atau tidak. Dengan hanya dua input, sistem memungkinkan empat kombinasi keadaan :

- Username benar, password benar
- Username benar, password salah
- Username salah, password benar
- Username salah, password salah

Keempat kombinasi ini dapat dianalisis secara matematis melalui tabel kebenaran untuk memverifikasi apakah logika autentikasi dirancang dengan tepat. Studi kasus ini tidak memasukkan faktor lain seperti OTP, token, biometrik, atau enkripsi, agar fokus analisis tetap pada struktur logika dasar autentikasi.

Selain pemodelan logika, metodologi juga mencakup implementasi simulasi autentikasi menggunakan bahasa C++ untuk menunjukkan bagaimana logika proposisional dituangkan ke dalam kode nyata dan memvalidasi kesesuaian antara model matematika dan implementasinya.

B. Perancangan / Pemodelan Matematika

Dalam tahap ini, proses autentikasi dipetakan menjadi suatu model logika proposisional. Dua proposisi utama didefinisikan sebagai berikut :

$A = \text{"username valid"}$

$B = \text{"password valid"}$

Keputusan autentikasi direpresentasikan sebagai proposisi majemuk:

$$C = A \wedge B$$

Artinya, autentikasi hanya dinyatakan benar apabila kedua proposisi A dan B bernilai benar. Untuk memverifikasi aturan autentikasi, tabel kebenaran disusun guna menggambarkan seluruh kombinasi nilai A dan B beserta keluaran C sesuai aturan logika. Tabel tersebut memungkinkan analisis menyeluruh terhadap berbagai kondisi autentikasi serta mendeteksi :

- a) kesesuaian antara logika sistem dan kebijakan autentikasi,
- b) skenario kesalahan seperti *false positive* (akses diberikan meskipun salah satu input tidak valid),
- c) skenario *false negative* (akses ditolak meskipun input valid).

Verifikasi matematis ini menjadi penting untuk memastikan konsistensi logika autentikasi, terutama ketika proses tersebut diterjemahkan ke dalam kode program. Model matematis ini kemudian digunakan sebagai acuan untuk implementasi simulasi C++ yang mengevaluasi input username dan password menggunakan logika $A \wedge B$.

Dengan metode ini, hubungan antara model logika dan implementasi praktis dapat diuji, sehingga validitas sistem

login dapat dipastikan baik secara teoretis maupun secara komputasional.

IV. HASIL DAN PEMBAHASAN

A. Analisis Menggunakan Tabel Kebenaran

Tabel 4. Tabel Skenario

Username (A)	Password (B)	Autentikasi (C = A $\wedge$ B)	Makna
1	1	1	Akses diberikan
1	0	0	Password salah, akses ditolak
0	1	0	Username salah, akses ditolak
0	0	0	Kedua kredensial salah

Dari tabel 4 terlihat bahwa tidak ada skenario di mana output akses bernilai benar kecuali kedua input benar, sehingga model logika konsisten.

B. Pemetaan Logika ke Kondisi Nyata pada Sistem Login

Model logika proposisional dapat dipetakan ke sistem login nyata sebagai berikut :

Tabel 5. Pemetaan logika ke kondisi nyata

Kondisi Sistem Nyata	Model Proposisi	Dampak Logis
Username cocok dengan database	A = True	Syarat awal autentikasi
Password cocok dengan hash	B = True	Syarat kedua autentikasi
Username salah	A = False	$A \wedge B = \text{False} \rightarrow$ akses ditolak
Password salah	B = False	$A \wedge B = \text{False} \rightarrow$ akses ditolak
Bug: akses diberikan meski salah satu salah	$A \wedge B$ tidak diterapkan	False positive (berbahaya)
Kedua salah	A = 0, B = 0	Aman: akses ditolak

Dengan pemetaan ini, kita dapat melihat potensi risiko jika implementasi kode tidak mengikuti logika $A \wedge B$ secara benar.

C. Implementasi Program Autentikasi Login (C++)

Berikut adalah simulasi program sederhana menggunakan logika yang sama dengan tabel kebenaran :

```
#include <iostream>
#include <string>
using namespace std;

bool autentikasi(string user_input, string pass_input) {
    string username = "admin";
    string password = "12345";

    bool A = (user_input == username);
    bool B = (pass_input == password);

    bool C = A && B; // Logika autentikasi (A ∧ B)
    return C;
}

int main() {
    string u, p;
    cout << "Masukkan username: ";
    cin >> u;
    cout << "Masukkan password: ";
    cin >> p;

    if (autentikasi(u, p)) {
        cout << "Login berhasil. Selamat datang!\n";
    } else {
        cout << "Login gagal. Username atau password salah.\n";
    }

    return 0;
}
```

Program ini secara langsung menerapkan logika $A \wedge B$ seperti yang disusun pada model matematis dan tabel kebenaran.

D. Hasil Akhir

Tabel berikut menunjukkan hubungan antara input pengguna dan hasil autentikasi:

Tabel 6. Hasil testing autentikasi

Skena-rio	A (User name)	B (Pass word)	Output Sistem	Status
1	Valid	Valid	Akses diterima	Benar
2	Valid	Tidak valid	Akses ditolak	Sesuai logika
3	Tidak valid	Valid	Akses ditolak	Sesuai logika
4	Tidak valid	Tidak valid	Akses ditolak	Sesuai logika

Hasil pengujian ini konsisten dengan tabel kebenaran sehingga logika autentikasi terverifikasi dengan benar.

V. KESIMPULAN

Penelitian ini menunjukkan bahwa tabel kebenaran merupakan alat verifikasi matematis yang sangat efektif dalam menganalisis dan memastikan konsistensi logika autentikasi pada sistem login. Dengan memodelkan proses autentikasi sebagai proposisi $A \wedge B$, seluruh kemungkinan

kombinasi input dapat dianalisis secara sistematis, sehingga memudahkan proses identifikasi terhadap kondisi yang semestinya menghasilkan akses maupun penolakan. Pendekatan ini membuktikan bahwa struktur logika formal mampu mendeteksi potensi kesalahan seperti false positive, yaitu kondisi ketika sistem secara keliru memberikan akses meskipun salah satu input tidak valid yang dapat menjadi celah keamanan serius pada sistem digital.

Pemetaan antara model logika dan kondisi autentikasi nyata membantu memperjelas implementasi aturan keamanan dalam sistem login berbasis username dan password. Selain analisis teoretis, implementasi program C++ yang disertakan pada penelitian ini memperlihatkan bagaimana logika matematika diterapkan secara langsung dalam kode program. Hasil pengujian menunjukkan bahwa implementasi praktis konsisten dengan model matematis, sehingga memperkuat validitas pendekatan logika proposisi dalam verifikasi sistem autentikasi.

Dengan demikian, penggunaan tabel kebenaran tidak hanya memberikan kerangka matematis yang kuat untuk memverifikasi logika autentikasi, tetapi juga berkontribusi terhadap peningkatan keamanan, keandalan, dan konsistensi sistem login.

Untuk penelitian selanjutnya, model autentikasi dapat dikembangkan ke arah mekanisme multi-faktor, seperti penggunaan OTP, autentikasi biometrik, token keamanan, serta integrasi teknik enkripsi modern agar sistem autentikasi menjadi lebih komprehensif dan tahan terhadap serangan siber.

DAFTAR PUSTAKA

- [1] R. Munir, Logika Proposisional dan Tabel Kebenaran, STEI ITB, 2008.
- [2] R. Munir, Penerapan Logika Proposisional dalam Sistem Komputasi, ITB, 2022.
- [3] J. C. Mitchell, "Foundations for Programming Languages and Systems," Journal of the ACM, vol. 45, no. 2, pp. 189–230, 1998.
- [4] D. Basin, C. Cremers, and C. Meadows, "Model Checking Security Protocols," Journal of Computer Security, vol. 19, no. 3, pp. 543–580, 2011.
- [5] J. A. Goguen, "Logic in Computer Science," ACM Computing Surveys, vol. 35, no. 2, 2019.
- [6] W. Stallings, Computer Security: Principles and Practice, 5th ed., Pearson, 2021.
- [7] A. Silberschatz, P. B. Galvin, and G. Gagne, Operating System Concepts, 10th ed., Wiley, 2020.
- [8] M. Bishop, Introduction to Computer Security, Addison-Wesley, 2018.
- [9] D. E. Denning, "A Lattice Model of Secure Information Flow," Communications of the ACM, vol. 19, no. 5, pp. 236–243, 1976.
- [10] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 2018.
- [11] ISO/IEC 27001, Information Security Management Systems — Requirements, ISO, 2022.
- [12] NIST, Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B), 2023.
- [13] M. Sipser, Introduction to the Theory of Computation, 3rd ed., Cengage Learning, 2013.
- [14] B. Schneier, Applied Cryptography, 2nd ed., Wiley, 2015.
- [15] K. Rosen, Discrete Mathematics and Its Applications, 8th ed., McGraw-Hill, 2019.