TUGAS AKHIR

SISTEM PERANGKAT LUNAK VERIFIKASI TANDA TANGAN DIGITAL MENGGUNAKAN SECURE HASH ALGORITHM 2 DAN ADVANCED ENCRYPTION STANDARD-256

Oleh:

Ahmad Zaky Nadimsyah 2024250039

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER DAN REKAYASA
UNIVERSITAS MULTI DATA PALEMBANG
PALEMBANG

2024

Fakultas Ilmu Komputer dan Rekayasa
Universitas Multi Data Palembang

Program Studi Informatika
Tugas Akhir Sarjana Komputer
Semester Gasal Tahun 2023/2024

SISTEM PERANGKAT LUNAK VERIFIKASI TANDA TANGAN DIGITAL MENGGUNAKAN SECURE HASH ALGORITHM 2 DAN ADVANCED ECMRYPTION STANDARD-256

Ahmad Zaky Nadimsyah 2024250039

Abstrak

Mudahnya proses pemindaian tanda tangan basah seseorang dapat menjadi potensi untuk di salah gunakan oleh pihak yang tidak berwenang sehingga dikembangkan lagi tanda tangan digital untuk mengatasi masalah ini. Tanda tangan digital digunakan untuk mengamankan pesan atau dokumen dari pihak yang tidak berhak atau berwenang. mengamankan data sensitif, menguatkan kepercayaan pihak yang menandatangan dan mendeteksi upaya perusakan. Solusi yang ditawarkan pada projek ini adalah pengembangan suatu sistem perangkat lunak yang mampu memverifikasi keaslian dokumen digital agar dokumen tidak disalahgunakan dan dapat digunakan sebagaimana mestinya menggunakan Fungsi Hash SHA-256 dan Algoritma Enkripsi AES-256. Perangkat lunak yang dihasilkan memiliki persentase kepuasan sebesar 93,71 % , sehingga dapat disimpulkan bahwa aplikasi yang telah dikembangkan dapat berjalan dengan baik.

Kata kunci: AES-256, Enkripsi, Dokumen Digital, Hash, SHA-2


UNIVERSITAS
MDP

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Jumlah informasi yang sangat banyak di internet yang telah menghubungkan banyak manusia membuat manusia kesulitan dalam memproses informasi tersebut karena begitu banyak hal yang harus dipertimbangkan, salah satunya adalah validasi kebenaran terhadap suatu informasi. Validasi informasi dibutuhkan untuk menentukan kebenaran suatu informasi, validasi bisa dilakukan dengan logika terhadap informasi tersebut atau bisa dilakukan dengan melihat sumber informasi. Validasi informasi sangat krusial dalam membantu pekerjaan, pemrosesan / pengolahan data-data penting sebagai bentuk layanan sebagaimana diharapkan oleh penerimanya.(Gunawan et al., 2022).

Urusan surat menyurat dilakukan diseluruh lapisan Masyarakat yang merupakan bagian dari negara Hukum pada urusan pekerjaan atau kegiatan sehari hari yang menyangkut mengenai kewajiban seorang Masyarakat secara hukum. Penandatanganan oleh semua pihak terkait wajib dilakukan dengan menandatangani dokumen dengan tanda tangan basah untuk mengikat maksud dan isi surat dengan semua pihak yang terkait sehingga memiliki nilai hukum. Tanda tangan basah dalam sebuah dokumen surat sudah diakui keabsahannya di mata hukum.(Sihombing, 2020).

Proses penandatanganan secara tradisional dilakukan dengan tinta basah oleh semua pihak pada suatu dokumen fisik, seiring berkembangnya teknologi yang

menuntut semua hal untuk lebih cepat munculnya tanda tangan elektronik yang diharapkan mampu menutupi kekurangan tanda tangan basah, dimana tanda tangan elektronik adalah tanda tangan basah yang di pindai sebagai citra digital dan bisa ditempelkan pada dokumen fisik dan dapat digunakan untuk mengkonfirmasi sebuah konten dalam sebuah dokumen. (Zubov, 2020). Mudahnya proses pemindaian tanda tangan basah seseorang dapat menjadi potensi untuk di salah gunakan oleh pihak yang tidak berwenang sehingga dikembangkan lagi tanda tangan digital untuk mengatasi masalah ini. Tanda tangan digital digunakan untuk mengamankan pesan atau dokumen dari pihak yang tidak berhak atau berwenang. mengamankan data sensitif, menguatkan kepercayaan pihak yang menandatangan dan mendeteksi upaya perusakan. (Zubov, 2020). Tanda tangan digital berisi informasi dokumen dan informasi pihak yang terkait, kedua hal ini disimpan secara aman umumnya kedalam *barcode* yang bisa ditempelkan pada dokumen digital sebagai wujud tanda tangan yang mampu membuktikan keabsahan suatu dokumen.

Tanda tangan basah mulai ditinggalkan seiring berkembangnya akses internet yang membuat peralihan infrastruktur kebutuhan surat menyurat mulai menjadi sistem *hybrid* dimana dokumen fisik masih diperlukan namun penanda tanganan dokumen bisa dilakukan secara elektronik. Hal ini membuat munculnya potensi pemalsuan tanda tangan elektornik karena tidak ada validasi yang bisa dilakukan terhadap suatu citra digital tanda tangan elektronik. Kasus pemalsuan tanda tangan basah maupun elektronik mulai bermunculan di instansi civitas akademik yang menguntungkan oknum tertentu dan merugikan pihak lainnya. Pada tahun 2014 kasus pemalsuan tanda tangan terjadi di Program Pascasarjana suatu

universitas (Ihwan, 2021) , selain itu di tahun 2016 kasus pemalsuan identitas dan pemalsuan tanda tangan dilakukan oleh warga yang menolak pendirian pabrik PT Semen Indonesia di daerah Rembang. (Tempo, 2016). Pada tahun 2017 dua orang dari *Indonesian Enterpreneur Club* (IEC) memalsukan stempel dan tanda tangan presiden badan eksekutif mahasiswa (BEM) di suatu Universitas. (Muria, 2017). Pada tahun 2022 mahasiswa suatu Universitas di lampung melakukan pemalsuan tanda tangan rektor di universitas tersebut untuk hak uji materi peraturan perundang undangan (Unila, 2022) dan pada tahun 2023 pemalsuan tanda tangan Gubernur Kalimantan Timur dilakukan oleh inspektorat daerah pada kasus izin usaha pertambangan. (Chalimah & Ridhuan, 2023).

Survei dilakukan untuk memperkuat argumen bahwa fenomena masalah pemalsuan tanda tangan terjadi di instansi civitas akademik di Kota Palembang. SMAN 18 Palembang dan SMKN 6 Palembang yang menerapkan urusan surat menyurat secara *hybrid* menggunakan tanda tangan elektronik menjelaskan bahwa memang pernah terjadi kasus penyalahgunaan tanda tangan namun menolak menyebutkan kapan, jumlah dan siapa pelakunya. SMA IBA Palembang dan SMK Ethika Palembang menyatakan bahwa mereka baru mau memulai untuk migrasi ke sistem hybrid untuk urusan surat menyurat namun menyadari bahwa nantinya penyalahgunaan tanda tangan bisa menjadi potensi masalah di waktu yang mendatang. Universitas Multi Data Palembang (MDP) mengklaim bahwa urusan surat menyurat sudah dilakukan secara *hybrid* yang menggunakan tanda tangan basah dan tanda tangan elektronik, tapi juga menyatakan bahwa untuk urusan dan

kebutuhan tertentu Universitas MDP menerbitkan tanda tangan digital sebagai wujud migrasi Universitas MDP ke *paperless transaction*.

Dari latar belakang masalah diatas, solusi yang ditawarkan pada projek ini adalah pengembangan suatu sistem perangkat lunak yang mampu memverifikasi keaslian dokumen digital agar dokumen tidak disalahgunakan dan dapat digunakan sebagaimana mestinya.

1.2 Rumusan Masalah

Dibutuhkan suatu sistem untuk memvalidasi keaslian dokumen digital.

1.3 Analisis Terhadap Batasan (*Constraint*)

1.3.1 Analisis dari Aspek Ekonomis

Rencana sistem perangkat lunak (SPL) yang anak dikembangkan dijelaskan kepada 5 organisasi, dimana setiap narasumber memiliki pendapat yang berbeda dari aspek ekonomis terkait SPL yang akan dikembangkan. Menurut Organisasi 1 yaitu SMAN 18 Palembang SPL yang akan dikembangkan diberi harga Rp 1.500.000. Menurut organisasi 2 yaitu SMKN 6 berpendapat bahwa SPL yang akan dikembangkan dapat dihargai Rp.1.300.000. Menurut organisasi 3 yaitu SMA IBA Palembang menyatakan bahwa mereka mengestimasi harga produk Rp. 1.500.000. Menurut organisasi 4 yaitu SMK Ethika Palembang mengestimasi bahwa SPL yang akan dikembangkan dihargai Rp.700.000. Menurut Organisasi 5 yaitu Universitas Multi Data Palembang mengestimasi harga produk ada diantara Rp. 1.000.000 sampai Rp. 2.000.000.

Selain *constraint* secara ekonomis yang disampaikan oleh 5 narasumber, dibutuhkan juga biaya untuk menunjang sistem perangkat lunak yang akan di*hosting* pada Amazon Web Service (AWS) sebagai penyedia layanan *cloud*. Jenis layanan yang akan digunakan adalah Elastic Compute Cloud (EC2) yang berupa layanan *Infrastructure as a Service* seharga 0.0464 $USD atau setara Rp. 726 / jam dengan spesifikasi yang ditunjukan oleh table 1.1.

Tabel 1.1 Spesikasi Perangkat *Virtual Machine*

Instance Type	vCPU	*Memory*	*Storage*
t2.*Medium*	2 *core*	4 GB	480 GB *Hard Disk*

Berdasarkan pendapat narasumber dan kebutuhan sistem perangkat lunak, produk yang akan dikembangkan memiliki tiga paket harga yang ditawarkan, dengan pembeda fitur halaman yang bisa diakses dan penyimpanan data, ketiga paket ini akan di jelaskan pada table 1.2.

Tabel 1.2 Paket Harga yang ditawarkan

No	Harga	Halaman	Penyimpanan Data
1.	Rp. 750.000	Verifikasi Dokumen	*Virtual Machine Internal Storage*, Dokumen yang telah diterbitkan akan dihapus setelah 30 hari
2.	Rp. 1.250.000	Verifikasi Dokumen & *List* semua	*Dedicated Database Service*, Dokumen yang

		Dokumen yang telah diterbitkan	telah diterbitkan akan dihapus setelah 180 hari
3.	Rp. 1.750.000	Verifikasi Dokumen & *List* semua Dokumen yang telah diterbitkan	*Dedicated Database Service*, Dokumen yang telah diterbitkan tidak akan dihapus dan akan diarsip setelah 365 hari

1.3.2 Analisis dari Aspek Manufakturabilitas

Tahapan ini dilakukan analisis dari aspek manufakturabilitas. Pada tahapan ini dilakukan wawancara dengan 5 civitas akademika di kota Palembang. Berikut merupakan hasil dari analisis dari aspek manufakturabilitas menurut narasumber yang telah diwawancari yang ditunjukkan pada tabel 1.3.

Tabel 1.3 Analisis dari Aspek Manufakturabilitas

Aspek	**SMAN 18**	**SMKN 6**	**SMA IBA**	**SMK Ethika**	**Universitas Multi Data Palembang**
Kemudahan dalam penerbitan dokumen yang sudah tertanda tangan secara digital (2 Bulan)	OK	OK	OK	OK	OK
Kemudahan dalam memverifikasi	OK	OK	OK	OK	OK

keaslian dokumen digital. (1 bulan)					
Total : 3 Bulan					

1.3.3 Analisis dari Aspek Sustainabilitas

Pada tahapan ini dilakukan analisis dari aspek sustainabilitas terkait perangkat lunak. Pada tahapan ini dilakukan wawancara dengan 5 civitas akademika di kota Palembang. Berikut merupakan hasil dari analisis dari aspek sustainabilitas untuk mengidentifikasi batasan perangkat lunak yang ditunjukkan pada tabel 1.4.

Tabel 1.4 Analisis dari Aspek Sustainabilitas

Aspek	**SMAN 18**	**SMKN 6**	**SMA IBA**	**SMK Ethika**	**Universitas Multi Data Palembang**
Sistem mampu menerbitkan dokumen digital yang sudah ditandatangan secara digital (10s)	OK	OK	OK	OK	OK

Sistem mampu memverifikasi keaslian dokumen digital (5s)	OK	OK	OK	OK	OK

1.4 Analisis Terhadap Karateristik Solusi

Tahapan ini dilakukan analisis dari aspek karakteristik solusi. Analisis karakteristik solusi dilakukan untuk menentukan solusi dari permasalahan yang ada dalam bentuk fungsi yang disediakan pada perangkat lunak. Tabel 1.5 merupakan hasil analisis terhadap karakteristik solusi.

Tabel 1.5 Analisis terhadap Karakteristik Solusi

No.	Masalah	Fungsi
1.	Potensi pemalsuan tanda tangan pada dokumen fisik.	Perangkat lunak mampu menerbitkan dokumen digital yang sudah ditandatangani secara digital.
2.	Kesulitan dalam menentukan apakah suatu tanda tangan pada dokumen fisik yang di pindai asli atau tidak.	Perangkat lunak mampu membuktikan integritas keaslian dokumen digital.
3.	Kesulitan dalam mendistribusikan dokumen	Perangkat lunak mampu menerbitkan dokumen digital yang bisa ditanda

	fisik ke banyak pihak yang bersangkutan.	tangani oleh banyak pihak yang bersangkutan, dan dokumen digital yang telah diterbitkan dapat diunduh sesuai kebutuhan.

1.5 Pemilihan Solusi dan Teknik

Penelitian oleh (Abraham et al., 2018) membahas mengenai pemanfaatan tanda tangan digital untuk mendukung program *Green Information and Communication Technology* (*Green* ICT), dengan bertujuan salah satunya adalah untuk mengurangi penggunaan kertas di lingkungan perkantoran. Metode yang digunakan adalah *Public Key Cryptographic Standard* #12, karena metode ini tidak memerlukan infrastruktur tersendiri sehingga dapat lebih menghemat biaya. Penelitian oleh (Saha, 2017) QR *Code* dan/atau *barcode* yang disematkan di dokumen pada dasarnya bukanlah tanda tangan digital dari dokumen, melainkan keduanya hanya media untuk menyimpan link yang akan mengarahkan ke alamat sistem untuk mengecek tanda tangan digital yang disimpan di dalam basis data sistem. Tanda tangan digital yang sebenarnya diterapkan adalah hasil perhitungan dengan fungsi *hash*. Penelitian oleh (Suratma & Azis, 2017) membahas mengenai penerapan tanda tangan digital menggunakan *Quick Response Code* (QR *Code*) dengan algoritma *Advanced Encryption Standard* (AES) pada dokumen permintaan barang. Tanda tangan digital diterapkan di dokumen permintaan barang. Penelitian oleh (Puspitasari & Permanasari, 2020) membahas mengenai penerapan algoritma Rivest-Shamir-Adleman (RSA) pada tanda tangan digital. Mekanisme

yang diterapkan yaitu dokumen terlebih dahulu dilakukan fungsi *hash* yang tidak sebutkan jenisnya sehingga menghasilkan *message digest*. *Message digest* yang dihasilkan kemudian dienkripsi menggunakan kunci publik dari algoritma RSA yang sebelumnya telah dibangkitkan terlebih dahulu bersama dengan pasangan kunci privatnya. Penelitian oleh (Nuraeni et al., 2018) membahas mengenai penerapan tanda tangan digital pada proses legalisasi ijazah. Mekanisme yang digunakan adalah algoritma RSA dan *Secure Hash Algorithm* (SHA)-512. Langkah pertama yang dilakukan adalah pembangkitan kunci publik dan kunci privat untuk proses *signing* menggunakan algoritma RSA. Setelah pasangan kunci dibangkitkan, langkah kedua adalah proses *hashing* menggunakan SHA-512 untuk menghasilkan *message digest*.

Solusi pendekatan pertama adalah *Digital Signature System* atau Dsign adalah sistem yang dikembangkan berbasis *Software as a Service* (SaaS), sistem ini mengimplementasi Fungsi SHA-1 untuk tanda tangan digital pada dokumen elektronik. (Saha, 2017). Solusi ini hanya menerapkan Fungsi *Hash* untuk integritas dokumen, namun tidak menerapkan enkripsi sama sekali. Solusi pendekatan kedua adalah sistem yang dikembangkan oleh (Suratma & Azis, 2017) melakukan penerapan tanda tangan digital menggunakan *Quick Response Code* (QR Code) dengan Algoritma *Advanced Encryption Standard* (AES) pada dokumen permintaan barang. Solusi ini hanya menerapkan enkripsi isi dokumen tanpa fungsi *hash* untuk menyembunyikan informasi pada dokumen tersebut. Solusi pendekatan ketiga adalah sistem yang dikembangkan oleh (Puspitasari & Permanasari, 2020) melakukan penerapan Algoritma RSA pada tanda tangan digital. Solusi ini

menerapkan fungsi *hash* dan enkripsi yang menggunakan *Assymetric Key* yang menghasilkan *Public Key* untuk kebutuhan enkripsi dan *Private Key* untuk kebutuhan dekripsi.

Pemilihan solusi dilakukan berdasarkan batasan masalah dan memilih atau mengkombinasikan alternatif solusi yang dijelaskan pada subbab ini. Pembuktian keaslian dokumen digital di civitas akademika membutuhkan agar sistem verifikasi dokumen digital bisa diakses oleh banyak orang, sehingga Algoritma RSA yang membutuhkan *private Key* untuk dekripsi *ciphertext* tidak cocok digunakan. Solusi pertama hanya menggunakan fungsi *Hash* untuk pencocokan dokumen tetapi tidak mengimplementasikan metode Enkripsi apapun. Solusi Kedua hanya menggunakan Algoritma AES untuk kebutuhan enkripsi tetapi tidak menggunakan fungsi *Hash* untuk isi informasi dokumen, sehingga alih alih membuktikan keaslian dokumen, Dekripsi pada Solusi kedua akan mengekspos isi dokumen tersebut yang bisa diakses secara *public*. Solusi yang diajukan untuk pengembangan projek ini adalah gabungan dari semua alternatif solusi yang telah dijelaskan, untuk mengurangi kelemahan masing masing alternatif solusi dan memperbaiki tingkat keamanan data serta mempermudah distribusi dokumen Digital. Solusi pada pengembangan projek ini akan menggunakan fungsi Hash SHA-256 untuk membuat *message digest* berdasarkan isi informasi penting dari dokumen, lalu mengenkripsi *message digest* tersebut menggunakan Algoritma AES dengan panjang *key* 256-*bit* dan memasukan nilai *ciphertext* yang dihasilkan ke dalam QR *Code*. *Key* yang digunakan untuk dekripsi dan enkripsi akan disimpan secara aman pada basis data dan nilai *Key* akan berbeda untuk setiap pihak yang memberi persetujuan pada dokumen digital.

1.6 Skenario Pemanfaatan Produk oleh Stakeholder

Produk dapat digunakan untuk membuktikan keaslian dokumen digital di civitas akademika dengan langkah langkah berikut:

1. Enkripsi Informasi Penting

   Produk mampu menenkripsi informasi perihal tujuan penandatanganan dokumen dan identitas penanda tangan.

2. *Generate* QR

   Informasi yang telah terenkripsi akan disimpan didalam QR-*Code* dan ditempel dengan dokumen digital.

3. *Scan* QR dan Dekripsi

   Produk mampu memindai dan mendekripsi informasi yang tersimpan.

4. Membuktikan keaslian dokumen digital

   Produk mampu menunjukan keaslian dokumen dengan Informasi Perihal tujuan penanda tanganan dokumen dan identitas penanda tangan. dengan mengikuti empat langkah diatas, dokumen digital tidak akan disalah gunakan dan dapat dipergunakan sebagaimana mestinya.

1.7 Tujuan

Tujuan dari pengembangan produk ini adalah mengembangkan perangkat lunak yang mampu menerbitkan dokumen digital dan secara aman mendistribusikannya serta mampu memverifikasi keaslian dokumen digital agar tidak disalah gunakan dan dapat digunakan sebagaimana mestinya.


UNIVERSITAS
MDP

DAFTAR PUSTAKA

Abraham, F. Z., Santosa, P. I., & Winarno, W. W. (2018). Tandatangan digital sebagai solusi teknologi informasi dan komunikasi (Tik) hijau: sebuah kajian literatur (Digital signature as green information and communication technology (Ict) solution: a review paper). *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *9*(2), 111. https://doi.org/10.17933/mti.v9i2.120

Chalimah, N., & Ridhuan, M. (2023). *Menunggu hasil kerja polisi urusi pemalsuan tanda tangan gubernur, penyidik sedang menyusun laporan terbaru*.KaltimPost.https://kaltimpost.jawapos.com/utama/01/02/2023/menunggu-hasil-kerja-polisi-urusi-pemalsuan-tanda-tangan-gubernur-penyidik-sedang-menyusun-laporan-terbaru

Gunawan, Rahmat, S., Yahya, W., & Seno. (2022). Rancang bangun sistem informasi verifikasi dan validasi data pengajuan tender berbasis web. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *16*(4), 11–19. https://doi.org/10.35969/interkom.v16i4.188

Ihwan. (2021). *Kasus pemalsuan tanda tangan di program pascasarjana UMI tahun 2014 , resmi dilaporkan oleh LSM gempa indonesia*.SulselBerita. https://sulselberita.com/2021/10/23/kasus-pemalsuan-tanda-tangan-di-program-pascasarjana-umi-tahun-2014-resmi-dilaporkan-oleh-lsm-gempa-indonesia/

Leurent, G., & Peyrin, T. (2020). SHA-1 is a shambles: first chosen-prefix collision on SHA-1 and application to the PGP web of trust. *Proceedings of the 29th USENIX Security Symposium*, 1839–1856.

M. Nasution, R. (2022). Implementasi metode secure hash algorithm (SHA-1) untuk mendeteksi orisinalitas file audio. *Bulletin of Computer Science Research*, *2*(3), 73–84. https://doi.org/10.47065/bulletincsr.v2i3.140

Muria. (2017). *IEC palsukan stempel dan tanda tangan presiden BEM UMK*.UMK. https://umk.ac.id/informasi/berita/2100-iec-palsukan-stempel-dan-tanda-tangan-presiden-bem-umk

NIST. (2022). *NIST retires SHA-1 cryptographic algorithm*.NIST. https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm

Nuraeni, F., Agustin, H., Muharam, I. M., Informatika, T., & Tasikmalaya, T. (2018). Implementasi tanda tangan digital menggunakan RSA dan SHA-512 pada proses legalisasi ijazah. *Konferensi Nasional Sistem Informasi (KNSI) 2018*, 864–869.

Puspitasari, D., & Permanasari, Y. (2020). Implementasi algoritma kriptografi Rivest Shamir Adleman (RSA) pada tanda tangan digital. *Prosiding Matematika*, *6*(1), 14–20. https://doi.org/http://dx.doi.org/10.29313/.v0i0.20771

Saha, G. (2017). DSign digital signature system for paperless operation. *2017 International Conference on Communication and Signal Processing (ICCSP)*. https://doi.org/10.1109/ICCSP.2017.8286370

Sihombing, L. B. (2020). Keabsahan tanda tangan elektronik dalam akta notaris. *Jurnal Education and Development*, *8*(1), 135. https://doi.org/https://doi.org/10.37081/ed.v8i1.1515

Suratma, A. G. P., & Azis, A. (2017). Digital signature using QR code by advanced encryption standard method. *Techno*, *18*(1), 59–68. https://doi.org/10.30595/techno.v18i1.1482

Tempo. (2016). *Kasus pabrik semen rembang, polisi usut kasus pemalsuan tanda tangan*.Tempo. https://koran.tempo.co/read/berita-utama-jateng/410502/polisi-usut-kasus-pemalsuan-tanda-tangan

Unila, R. (2022). *Tanggapi kasus tanda tangan palsu, rektor ingatkan mahasiswa taat aturan*.UNILA. https://www.unila.ac.id/tanggapi-kasus-tanda-tangan-palsu-rektor-ingatkan-mahasiswa-taat-aturan-2/

Zubov, V. V. (2020). An electronic signature within the digital economy. *Proceedings of the II International Scientific Conference GCPMED 2019 - "Global Challenges and Prospects of the Modern Economic Development,"* 621–625. https://doi.org/10.15405/epsbs.2020.03.89