IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Novel Hybrid Algorithm For an Efficient Data Security Over Wireless Transfer

S Susila Sakthy[#1], Rubankumar S[#2], Sahil Ram R[#3]

[#1] Assistant Professor, Department of Information Technology

[#2] [#3] Student, Department of Information Technology

[#1] [#2] [#3] Sri Sairam Engineering College(Autonomous), West Tambaram, Chennai – 600044.

Affiliated to Anna University, Tamil Nadu, India.

- ***Abstract***- **Data security refers to the process of protecting data from the unauthorized access and data corruption throughout its lifecycle. To overcome this problem this project presents an Efficient Data Security System for where two security algorithms will be merged to secure the data stored and accessed in cloud. In addition, the emerging block chain technology with the wireless data transfer system, makes easy the interaction between the data and cloud. A frontend framework is developed using Reactjs framework where the data is entered for analyzing which will undergo the process of encryption using the hybrid secure algorithm. This is been stored securely in the cloud database such as mongo DB as an highly secure encrypted key. Whenever the data is requested, then the key is received from the database and decrypted using in the frontend to view the original data.**

Keywords

JSON Web Token, Cipher AES, SHA 256

I. Introduction

This project is to ensure secure transmission of data over a wireless communication. To design an efficient system where data is secured by merging two security algorithms for data stored and accessed in cloud. To design a web application for entering and viewing data for encryption. Organizations around the globe are investing heavily in information technology (IT) cyber security capabilities to protect their critical assets. Whether an enterprise needs to protect a brand, intellectual capital,

Pros:

and customer information or provide controls for critical infrastructure,

the means for incident detection and response to protecting organizational interests have three common elements: people, processes, and technology.

II. Literature Survey

1. **Jun Shang, Maoyin Chen, Member, IEEE, and Tongwen Chen, Fellow, IEEE," Optimal Linear Encryption Against Stealthy Attacks on Remote State Estimation"**

Defending against malicious attacks has become increasingly important in various cyber-physical systems. This paper presents an encryption-based countermeasure against stealthy attacks on remote state estimation. Smart sensors transmit data to a remote estimator through a wireless communication network, in which data packets can be intercepted and compromised by attackers. The remote end is equipped with a false data detector that monitors the system. To avoid being detected, the attack should follow the stealthiness constraint. A linear encryption scheme is proposed to reduce the influence of potential stealthy attacks. For arbitrary linear encryption, the worst-case linear attack that yields the largest estimation error is derived. Accordingly, the optimal linear encryption, which minimizes the worst-case estimation error, is designed based on the Stackelberg game analysis. The above optimal strategies are considered in both the complete and partial measurement information scenarios for the attacker. Moreover, the generalization to nonlinear encryption strategies is also discussed. Comparisons of attack and encryption strategies through numerical examples are provided to illustrate the theoretical results.
Comparisons of attack and encryption strategies through numerical examples
are provided to illustrate the theoretical results.

Cons:
It is not suitable for encryption and decryption based application.

2. **A Blockchain -based Water Control System for the Automatic Management of Irrigation Communities, Borja BORDEL, Diego MARTIN, Ramón ALCARRIA and Tomás ROBLES [2019]**

Borja BORDEL, Diego MARTIN, Ramón ALCARRIA and Tomás ROBLES (2019) has observed that Irrigation communities, especially in rural areas whose economy depends on agriculture, face a critical problem with the increasing water crisis. In this paper it is proposed a water control system to efficiently manage and coordinate the use of water in these communities. Blockchain technologies are employed to support trust among community members and commercial resource constrained devices communicating with the Blockchain network compose the hardware platform. A first implementation of this system and an evaluation of the system's performance are also presented. In this paper they proposed a water control system for irrigation communities, which must share a water source or quota. The solution employs Blockchain networks to make a group of independent users, competing for scarce resources, to trust the system and the other community members. At hardware level, electronic devices and computing nodes support the control operations. As conclusion, a control system based on Blockchain and electronic devices is adequate in this environment, thanks to the ability of Blockchain to provide trust.

Pros:

A control system based on Blockchain and electronic devices is adequate in this environment, thanks to the ability of Blockchain

to provide trust.

Cons:

The results show that the water control system is not very secure.

3. Caio Davi, Andre Pastor, Thiego Oliveira, Fernando B. de Lima Neto, Ulisses Braga-Neto, Abigail W. Bigham, Michael Bamshad, Ernesto T. A. Marques, Bartolomeu Acioli-Santos,"Severe Dengue Prognosis Using Human Genome Data and Machine Learning"[2020]

Caio Davi, Andr´e Pastor, Thiego Oliveira, Fernando B. de Lima Neto, Ulisses Braga-Neto, Abigail W. Bigham, Michael Bamshad, Ernesto T. A. Marques, Bartolomeu Acioli-Santos.(2019) has evolved that Dengue has become one of the most important worldwide arthropod-borne diseases. Dengue phenotypes are based on laboratorial and clinical exams, which are known to be inaccurate. We present a machine learning approach for the prediction of dengue fever severity based solely on human genome data. Methods: One hundred and two Brazilian dengue patients and controls were genotyped for 322 innate immunity Single Nucleotide Polymorphisms (SNPs). Our model uses a Support Vector Machine (SVM) algorithm to find the optimal loci classification subset, and then an Artificial Neural Network (ANN)is used to classify patients into dengue fever (DF) or severe dengue (SD). Results: The ANN trained on 13 key immune SNPs selected under dominant or recessive models produced median values of accuracy greater than 86%, and sensitivity and specificity over 98% and 51%, respectively. The proposed classification method, using only genome markers, can be used to identify individuals at high risk for developing the severe dengue phenotype even

APR'2021

in uninfected conditions. Our results suggest that the genetic context is a key element in phenotype definition in dengue. The methodology proposed here is extendable to other Mendelian-based and genetically influenced diseases.

Pros:

This method is extendable to other Mendelian-based and genetically influenced diseases.

Cons:

The SVM algorithm is not suitable for large datasets.

4. Chained Compressed Sensing: A Block-Chain-inspired Approach for Low-cost Security in IoT Sensing, Mauro Mangia, Member, IEEE,, Alex Marchioni, Student Member, IEEE,, Fabio Pareschi, Member, IEEE,Riccardo Rovatti, Fellow, IEEE,, Gianluca Setti, Fellow, IEEE [2019]

Mauro Mangia, Member, IEEE,, Alex Marchioni, Student Member, IEEE,, Fabio Pareschi, Member, IEEE,, Riccardo Rovatti, Fellow, IEEE,, Gianluca Setti, Fellow, IEEE have proposed Chaining, i.e., the mode of operation in which each message is encrypted considering a digital summary of previous ones, is here applied to block-cipher stages based on compressed sensing. We show that this simple and parsimonious technique may significantly harden the resulting system with respect to common threats such that ciphertext-only, known plaintext, and man-in-the-middle attacks. Non negligible robustness comes at the price of not more than a 2% of energy overhead with respect to the pure compression stage which represents a 24× reduction with respect to straightforward implementation of a traditional cryptography primitive like AES and gives recommendations on the introduction of Blockchain technology into modern banking systems.

Pros:

Uses high-end algorithms like AES.

Cons:

The AES algorithm uses a too simple algebraic structure, making it vulnerable to hacking.

5. Junqin Huang, Linghe Kong, Senior Member, IEEE, Guihai Chen, Min-You Wu, Xue Liu, Senior Member, IEEE, Peng Zeng, "Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism" [2019]

Junqin Huang, Linghe Kong, Senior Member, IEEE, Guihai Chen, Min-You Wu, Xue Liu, Senior Member, IEEE, Peng Zeng have proposed Industrial Internet of Things (IIoT) plays an indispensable role for Industry 4.0, people are committed to implementing a general, scalable and secure IIoT system to be adopted across various industries. However, existing IIoT systems are vulnerable to single

point of failure and malicious attacks, which cannot provide stable services. Due to the resilience and security promise of blockchain, the idea of combining blockchain and IoT gains considerable interest. However, blockchains are power-intensive and low throughput, which are not suitable for power constrained IoT devices. To tackle these challenges, we present a blockchain system with credit-based consensus mechanism for IIoT. We propose a credit-based proof-of-work (PoW) mechanism for IoT devices, which can guarantee system security and transaction efficiency simultaneously. In order to protect sensitive data confidentiality, we design a data authority management method to regulate the access to sensor data. In addition, our system is built based on directed acyclic graph (DAG)-structured blockchains, which is more efficient than the satoshi-style blockchain in performance. We implement the system on Raspberry Pi, and conduct a case study for the APR'2021

smart factory. Extensive evaluation and analysis results demonstrate that credit-based PoW mechanism and data access control are secure and efficient in IIoT.

Pros:

The results demonstrate that credit-based PoW mechanism and data access control are secure and efficient in IoT

Cons:

In this system DAG is used, no node in the graph can reference back to itself.

III. Existing System

1. Lightweight Directed Acyclic Graph(DAG) based Blockchain(LDV) is used.

2. This method is adopted to address the storage challenge existing in VSNs.

3. Experimental results show that LDV can save 97.13% of storage space and has good scalability.

4. System securely transmit sensor data over a wireless communication network.

5. The sensor data is transmitted in packets that is secured using the encryption algorithm.

6. A linear encryption scheme is used to secure the data packets sent through wireless communication network.

Drawbacks:

1.It A single encryption algorithm is insufficient to transmit data securely.

2.The system can be easily hacked.

3.Cannot secure highly confidential data.

IV. Proposed system

1. A novel hybrid algorithm for data security is proposed.
2. An encryption such as JWT, block chain security such as cipher AES and blockchain SHA-256 Hash algorithm is proposed to secure the data in storage and data transmission.
3. A Reactjs framework is used to develop the frontend by which the data can be stored and resumed.
4. On the server side the data is secured using hybrid secure algorithm where it is collected and processed and data is stored in the database.
5. This un hackable key is again used at the user end to decrypt the data.

Merits:

1. An end-to-end data security is provided by hybrid secure algorithm.

2. Ensures security over the wireless data transfer server to the database.

3. It can be used in all applications where data is transferred wirelessly.

4. Bank and hospital details can be secured with at most security.

A. JSON Web Token Generation

1. JSON Web Token is an Internet standard for creating data with optional signature and/or optional encryption whose payload holds JSON that asserts some number of claims.

2. The tokens are signed either using a private secret or a public/private key. **3.** The tokens can be signed by one party's private key (usually the server's) so that party can subsequently verify the token is legitimate.
4. If the other party, by some suitable and
APR'2021

trustworthy means, is in possession of the corresponding public key, they too are able to verify the token's legitimacy.
5. The tokens are designed to be compact, URL-safe, and usable especially in a web browser single-sign-on (SSO) context.

B. JSON Web Token to Cipher Generation

1. JSON Web Token (JWT) is an Internet standard and the data will be created with optional signature or optional encryption and payload holds JSON that asserts some number of claims.
2. JWT is converted and generated into a cipher using crypto AES algorithm.
3. Advanced Encryption Standard (AES) is a block cipher, i.e., a method for encrypt and decrypt information then Whenever files are transmitted over secure file transfer protocols like HTTPS, FTPS, SFTP, Web DAVS, OFTP or AS2, the data will be encrypted by either AES 256, 192, or 128.

C. Merging of Cipher and SHA-256

1. SHA-256 is a set of cryptographic hashing function, they are built using the Merkle Damgard structure, from a one way compression function itself built using the Davis-Meyer structure from a specialized block cipher.
2. The cipher algorithms are then merged with sha 256 which is nothing but a hash function.
3. The Protocol works with information broken down into pieces of 512 bits (or 64 bytes in other words). It produces its cryptographic "mixing" and then issues a 256-bit hash code. The algorithm includes a relatively simple round, which is
repeated 64 times.

D. Node API Generation

1. An application programming interface (API) is a computing interface and it interacts between multiple software intermediaries.
2. NodeJS is an open-source, cross platform, back-end and JavaScript runtime environment that executes the JavaScript code outside a web browser. NodeJS lets the developers use
JavaScript to write command line for server-side scripting—running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser.
3. Consequently, NodeJS represents a "JavaScript everywhere" paradigm, unifying web-application development around a single programming language, rather than different languages for server- and client-side scripts.

E. Database Integration

1. In this project, Mongo DB is used for database integration. MongoDB is an object-oriented database and it is simple ,scalable and dynamic .
2. It is based on the NoSQL document mode and it will be stored.
3. The data objects are stored as a separate document inside the
collection and the data are stored in columns and rows of a traditional relational database.

F. Web Application Development

1. A web application using a javascript framework, reactJS will be developed from which data is transmitted over a wireless communication.
2. React (also known as React.js or ReactJS) is an open-source, front end, JavaScript library for building user interfaces or UI components.
3. It is maintained by Facebook and a community of individual developers
APR'2021

and companies. React can be used as a base in the development of single-page or mobile applications.

V. System architecture

The working of the total model from the above diagrams can be explained as follows. The medical data to be secured is given through a web application which is converted to the JSON format, that is to be secured and encrypted is first converted to a token using a HS-256 algorithm, with an inbuilt secret key. This token is then encrypted to a cipher text using a crypto AES algorithm, with an inbuilt secret key. These two

secret keys from the JWT and crypto AES algorithm are converted to a hash key using a blockchain algorithm SHA-256 algorithm. This hash key is then embedded with the cipher text which is nothing but the end output of the encryption process. This medical data is sent from a reactJS web application to a mongoDB database through API which is developed using nodeJS. The data secured through block chain can never be decrypted it can only be encrypted using the hash key of another member of a network. Thus, the project has successfully ensured secure data transfer over wireless communications.

APR'2021

Figure 5.2 Decryption of original data

VI. Final Results Obtained

A web application using a javascript framework reactJS was successfully developed, to enter the patient details to perform diagnosis for diabetes.

The below screenshot shows the web application for the project

Figure 6.1 Hybrid data security login page

The user enters his/her login credentials to enter into the webpage.

The below screenshot shows the user entering his/her login credentials:

Figure 5.1 User-end & back-end system architecture

Figure 6.2 Sign-In page

Once the user has successfully logged in, the home page is displayed to the user. The patient enters his/her medical details to be used to perform encryption. On clicking the save location button, the location is saved. The below screenshot shows the form onto which the user uploads the medical data:

Figure 6.3 Homepage

After filling the details the encrypted result of the filled data is displayed and stored in the server securely using the hybrid secure algorithms.

The below screenshot shows the user saving the details to be kept secure:

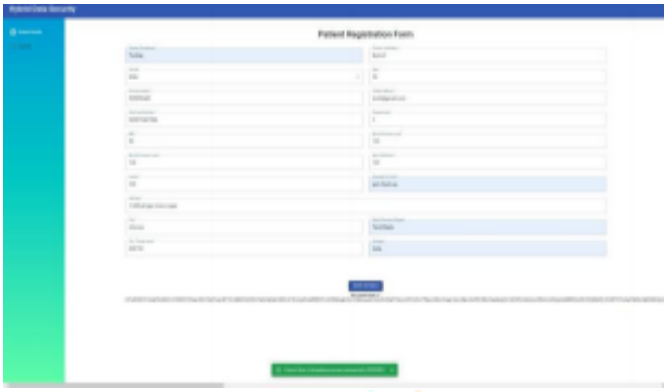

Figure 6.4 Details saved onclick

The saved location can be viewed on the patient details tab.
The below screenshot shows the user saved patient details:

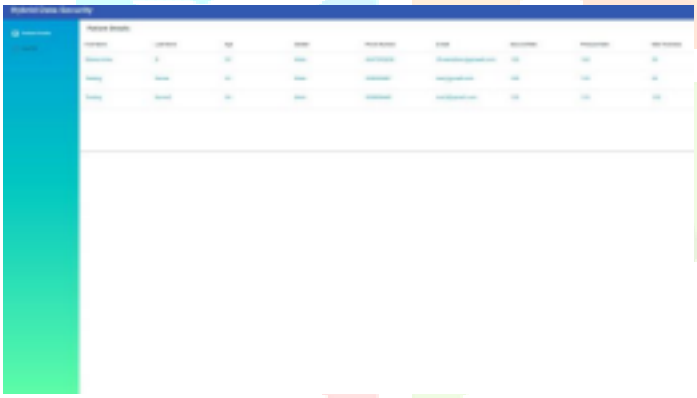

Figure 6.5 Saved patient details

On clicking the view button in patient details tab of a specific patient, the specific medical data of the patient is displayed.

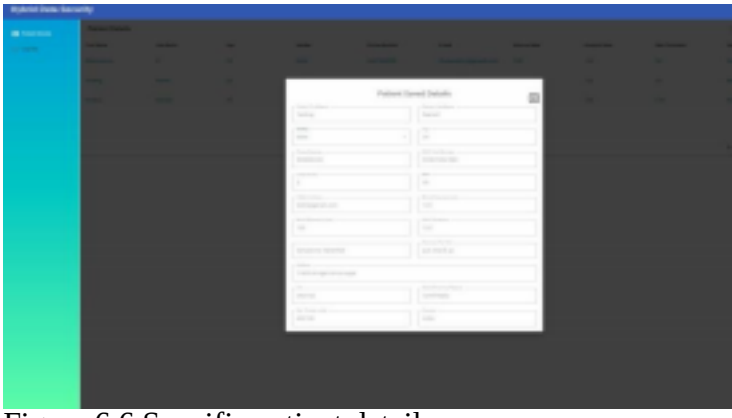

Figure 6.6 Specific patient details
The below image of the graph shows that each data query takes about 100 to 200m

Figure 6.7 Graph

Thus, from the above results and discussion, it is clear that we have efficiently made a project for successfully securing the data to be transmitted through wireless communications with a web application developed using a javascript framework ReactJS to encrypt and send medical data of a patient through wireless communications . Thus, we have successfully implemented the scope of the project.

VII. Conclusion

This project is used to provide a solution to perform securely transmit data through a wireless communication medium using a web application developed using a javascript framework reactJS. By this project, we can protect data from unauthorized access. Thus, this project provides an affordable and efficient means to protect and preserve data.

VIII. References

[1] Jun Shang, Maoyin Chen, Member, IEEE, and Tongwen Chen, Fellow, IEEE,"Optimal Linear Encryption Against Stealthy Attacks on Remote State Estimation" ,[2020]
[2] Novel Hybrid CMOS/Memristor Implementation of the AES Algorithm Robust against Differential Power Analysis Attack, Massoud Masoumi,[2019]

[3] An Enhancement of Data Encryption Standards Algorithm (DES), Nadia Mustafa Mohammed Alhag University of Gezira Faculty of Mathematical Sciences and Computer Medani,[2018]
[4] Ensuring Data Security in Databases Using Format Preserving Encryption, Shikha Gupta1 , Satbir Jain3 Computer Engineering NSIT New Delhi, India,[2017]
[5] Enabling Authorized Encrypted Search for Multi-Authority Medical Databases,Lei Xu, Shifeng Sun, Xingliang Yuan, Joseph K. Liu, Cong Zuo, Chungen Xu*[2016]
[6] Chained Compressed Sensing: A Block-Chain-inspired Approach for Low-cost Security in IoT Sensing, Mauro Mangia, Alex Marchioni, Fabio Pareschi, \Riccardo Rovatti, Fellow, IEEE,Gianluca Setti, Fellow, IEEE, 2019