Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 4, August 2021, pp. 2263~2272
ISSN: 2302-9285, DOI: 10.11591/eei.v10i4.2918

Design a mobile application for vehicles managing of a transportation issue

Seddiq Q. Abd Al-Rahman[1], Sameeh Abdulghafour Jassim[2], Ali Makki Sagheer[3]
[1]University of Anbar, Department of Computer Networks Systems, Anbar, Iraq
[2]Department of Vocational Education, General Directorate of Education in Anbar, Ministry of Education, Iraq
[3]Al-Qalam University College, Kirkuk, Iraq

Article Info

Article history:

Received Feb 25, 2021
Revised May 1, 2021
Accepted May 27, 2021

Keywords:

Cryptography
Mobile application
Transportation
Web database

ABSTRACT

The movement of people between cities is leading to a recovery in the economy that transportation companies have begun to dominate. These companies start providing the best services to customers and promoting them through workers to earn money properly. From this basis, this paper presents a system designed to manage a company that transports people and goods between a group of cities. Database management was used across the web to enable data exchange between workers. The database is designed to be accessible to workers. It has also been suggested that the elliptic curve can be used to generate public and private keys for all parties while the company's management generates a prime number every day to ensure the confidentiality of the exchanged data. In this proposal, the rivest-shamir-adleman (RSA) algorithm is used to encrypt transferred data. It uses technology to exchange information if the recipient is not connected to the network. The proposed system performs a good service for the company's management in securing the transferred data where smartphone applications are designed to work on it.

Corresponding Author:

Seddiq Q. Abd Al-Rahman
Department of Computer Networks Systems
University of Anbar, Ta'mim, Ramadi, Anbar, Iraq
Email: co.sedeikaldossary@uoanbar.edu.iq

1. INTRODUCTION

Many systems of traditional communication have been replaced by the internet because of its important uses with suitable cost and usability. Users of the internet are in danger of being attacked as they share information daily [1]. Nowadays, many services like money exchange and data sharing are done online. Although this seems easy, it puts the users in danger as there are many security concerns. As soon as the user shares information via a wireless network, the information can be attacked. Data sniffing is one of these attacks where data shared can be attacked and compromised by a third party [2], [3]. Moreover, network administrators can view, analyze, and store the transmitted information of the user with the help of commercial products [4].

The need for securing the internet from the attackers has increased with the increase of the need for transferring data via the internet. Data secrecy tools like cryptography and steganography are now used to secure the transferred data [5], [6]. Cryptography helps to send messages in a way that attackers cannot read or understand it as this tool jumbles the message. In this way, only the intended recipient can read and understand it. Cryptography depends on algorithms that are considered symmetric and asymmetric [7], [8]. According to symmetric algorithms, the sender and the receiver apply a single secrete key during communicating. These algorithms use what is so-called single-key and secrete-key encryption. The

computational cost of this technique is relatively small. Also, exchanging, non-repudiating and authenticating keys show difficulty [9], [10]. Asymmetric algorithms implement two separate keys. Messages are encrypted by a public key. Another private key is used in decrypting the received messages [11]. Mathematical complications can be solved by using asymmetric algorithms to make their state irreversible. Numbers factoring is the one obtaining it as the prime number of products. This is used to help generate pair keys [12], [13]. The encrypting mechanism can be provided by many solutions to ongoing data to exchange packets between two parties. Despite this encryption, there are still security concerns like reply attacks. The attacker can use and send pre-validated packets back to the user which can disturb and confuse the communication. So, it is so important to secure transferring and storing data [14].

Since it can implement and store data, the web is used in all procedures today. Although the web is open and flexible, data publishers, and data consumers face challenges lake the way data are presented, and described represent, describe, and make data available in an easy and understood way [15], [16]. Unlike conventional databases that have a single data model of data management and access, the web has multiple modules of data access, and management. Some data should not be shared openly. Individual's privacy, security, and commercial sensitivity are to be protected. It is the data publishers' job to determine what data can be shared [17]. Assessing the data exposure risk and the way the best way of data protection is the job of data sharing policies like authorization and authentication of data [18], [19]. Sensitive information includes home address, full name, national identification number, email address, internet protocol (IP) address, face, credit card numbers, birthplace, login name, and health records [8]. Although it seems that one can share information openly in certain controlled environments, publishers are to be aware that collecting data from different resources put the user's information at risk of being attacked [17], [20].

The rest of this paper is organized is being as; first provide the short introduction, thereafter section 2 related works. Then, section 3 discussed the proposed system, while section 4 displays the results. After that, section 6 describes the conclusion and future work ideas.

2. RELATED WORKS

Recently, securing systems in any company management has gained much awareness and concern. The most serious studies similar to the proposed system are mentioned as:

- Chen *et al.* [21] suggested a safe and efficient approach to blockchain-based data trade and data exchange between them. They propose a general blockchain-based data trading framework for the internet of vehicles. The authors were able to implement an algorithm to secure the exchange of information and money among vehicle users. They relied on the elliptic curve to achieve better data security and they also created a database that included the movement of vehicles. The results were good in terms of data storage and vehicle movement determination.
- Kushwah *et al.* [22] used the elliptic curve to identify the digital signature of car owners and their data. The authors proposed the elliptic curve digital signature algorithm (ECDSA) based on message authentication in the vehicular network model. Their proposed framework is capable to gain higher security and provide greater safety to the vehicles in transferring the message.
- Jitha and Kumar [23] suggested a way to secure the data transferred in the short message service, (SMS). The RSA algorithm was used to generate and publish keys, while the advanced encryption standard (AES) algorithm was used to secure the message in encryption and decryption. The proposal was implemented in the Android operating system for smartphones. The encryption was associated with only two users and there is no data traffic control center. The results of the work were clear in terms of data security.
- Lin *et al.* [24] suggested a secure data transmission mechanism that embeds the elliptic curve cryptosystem into the vehicle. The study is based on encrypting data transferred between vehicles using the elliptic curve to generate keys and encryption/decryption texts. The encrypted texts move between a group of vehicles and management. The data transferred between the vehicles is not stored and the management cannot control the generation of keys or the times of data transfer or storage. The study relied on the elliptic-curve diffie-hellman (ECDH) protocol to compute a common session key to secure each other information along the transmission path. The study obtained good results in coding inside the elliptic curve in terms of the time of secure data transmission and group key synchronization.
- Prathama *et al.* [25] suggested an implementation scheme with the mobile payment process in Indonesia. The study used the elliptic curve for encryption/decryption data. The system designed with mobile applications has the power and security of the transferred data. The proposed system has achieved results in terms of privacy protection, authentication. The study lacks the identification of a body to manage work within the system and control the movement of funds.

There is a research gap as there is a lack of works on methods for transportation issue management with the handle of workers and customers. As a result, the purpose of the paper is to provide a system that manages work between the company's management and workers through mobile applications. This is done by exchanging messages between workers and storing them in the web database. So, it is secured through the system. To achieve the specified main objectives, the research questions were defined as:
Q1: How to exchange data between workers?
Q2: How to secure the transferred data? And how is the management control securing it?
Q3: What is the best way to store data on the web and how is it done?

3. IMPLEMENTATION OF PROPOSED SYSTEM

The scenario of the proposed system is based on three important pillars: Data traffic management, data security, and work management between the workers. Therefore, it requires the presence of a specific and secure place to store the transferred data in a way that can be accessed by the management of the company and the receiving worker. A better place must be provided for all to be the basis of dealing with data and preservation. It will be referred to later to rely on it in taking appropriate decisions. Data stored online allows many to access it through sharing links, but maybe more vulnerable to attackers. On this basis, the proposed system depends on securing the data exchanged between the company's management and the dealers on hybridizing heterogeneous encryption algorithms. Asymmetric encryption has two keys, one is public, and the other is private. Anyone who is allowed to enter the system can see all the keys declared for workers and can also use them. Attackers will not be able to know the original text of the message due to the difficulty in speculating the key to the encryption. The process of storing and encrypting data is the responsibility of the company's management, which controls all joints of the proposed system. The proposed system was designed to be easy to deal with workers through mobile applications that were designed. The administration must have a computer program to be able to manage the process. The work of the proposed system can be represented in Figure 1 (a). The movement of data within the proposed system begins daily from the hour (00:00:00) that the administration carries out. The administration sends the prime number used to generate the keys and encryption operations directly to the workers. Then the workers generate the public and secret keys and send them to the database. The movement of keys within the proposed system is within Figure 1 (b).

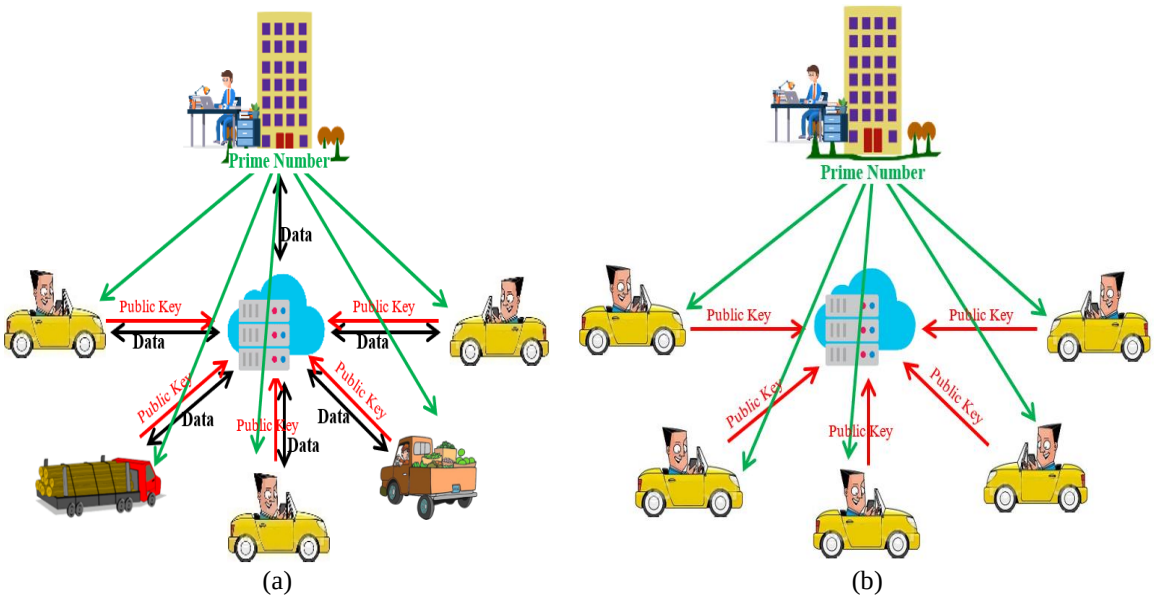


Figure 1. These figures are; (a) the scenario of the proposed system, (b) the movement of keys in the proposed system

Website reservation companies provide services to their users through the method of securing their users' data and the speed of transferring and exchanging all data. Therefore, the place where reserved sites and services are reserved plays an important role in providing data and analysis services. The schema used to

link spreadsheets is also very important for easy access to what it wants. The schema star was used in the system database that was cached through the company's online storage space. The database includes the worker information table, system login table, table of public keys for workers, and table for exchanging messages exchanged between parties. These tables ultimately lead to an optimal analysis of the movement of data between workers and their whereabouts, as well as identifying the most active centers. Below is an explanation of all the essentials of the proposed system in managing the operation of the passenger carrier.

3.1. Management system

In the proposed system, the system administration performs several tasks, including controlling the number of workers and generating keys, the initial numbers for encrypting, and decrypting data daily. The administration also cuts communication between the workers at the end of each day, for the sake of safe transmission of texts properly. It is the responsibility of the administration of the proposed system to distribute the work equally among workers, as well as to know the largest movement of workers, and beneficiaries of the system and their locations.

The proposed system was designed to meet the needs of the private carriers for peoples. Such companies deal with a specific number of workers based on specifications for their selection. After selecting the workers, they will be distributed in the locations of their need to fill all areas of the population with their services. The data of workers and their location, in addition to their vehicle specifications and other information, is entered into a database. The data entering the database is cleaned in terms of typing error and redundancy to benefit from it over time for decision making. Data is cleaned by using the extract transform load (ETL) algorithm. The data is stored directly on the company's server site within a database whose tables are designed and joints by the table's schema.

The responsibility of the management controls the movement of information within the system and the presence of workers in the branches and centers of the company. The administration must know the data movement within the proposal. The management is to make copies of the messages circulated among workers as backup copies thereof. The management periodically cuts communication between workers to generate a prime number. This takes place in the middle of the night when the traffic between all two workers is zero. The benefit of this is to regenerate the keys and cut the roads on the attackers as well as for statistical work through which profits and losses can be calculated and reallocated in the centers as an activity. Reports are prepared according to mathematical operations to take the appropriate decision to reopen more than one center for the most interacting areas or drown the centers in the inactive areas.

In our proposed system, the prime number is used in the process of generating the encryption key and the decryption key as well as in the encryption and decryption processes. So, the generation of the number is the main pillar of this proposal. The prime number should consist of a minimum of 19 digits and a maximum of 24 digits. So, the first prime number that can be obtained will be (1000000000000000003) and the last prime number that can be obtained is (9944496698899994966989999). Always note in these numbers, the presence of prime numbers is small when increasing the digits of the number. The number is generated randomly within the proposed system management every day at (00:00:00) and automatically. The generated number is sent to all workers' devices individually and is not stored within the database. It is possible to repeat the prime number between groups of days in a certain period. Thus, this does not affect the performance of creating the keys or the encryption process because the processes take numbers within belonging to the group *GF(p)*. The main reason for selecting the size of the prime number is to maintain the security of the system and the integrity of its information from the attackers.

3.2. Sending information between workers

One of the most important processes carried out by the proposed system is the exchange of information between workers and management. So, the workers inside the system will not be connected with the local server, they are connected with the reachable and unreachable remote server because of the cable connection or other problems of connection. In this mode, workers are allowed to keep using the system when an immediate confirmation is not necessary. All the queue messages are transmitted on it as soon as the remote server gets connected. The queue of the stored information stays for 15 minutes only. If the client is not connected, the messages will be deleted and return a message to the sender for reject. So, it will go under Figure 2(a). The user can either send data as a text or as a large data file as soon as the system is logged into by the user. This distinction is presented depending on the size of data as they, during the process of exchanging, do not use the same line. Figure 2(b) presents the transactions of the system of exchanging the message through the sequence diagram.

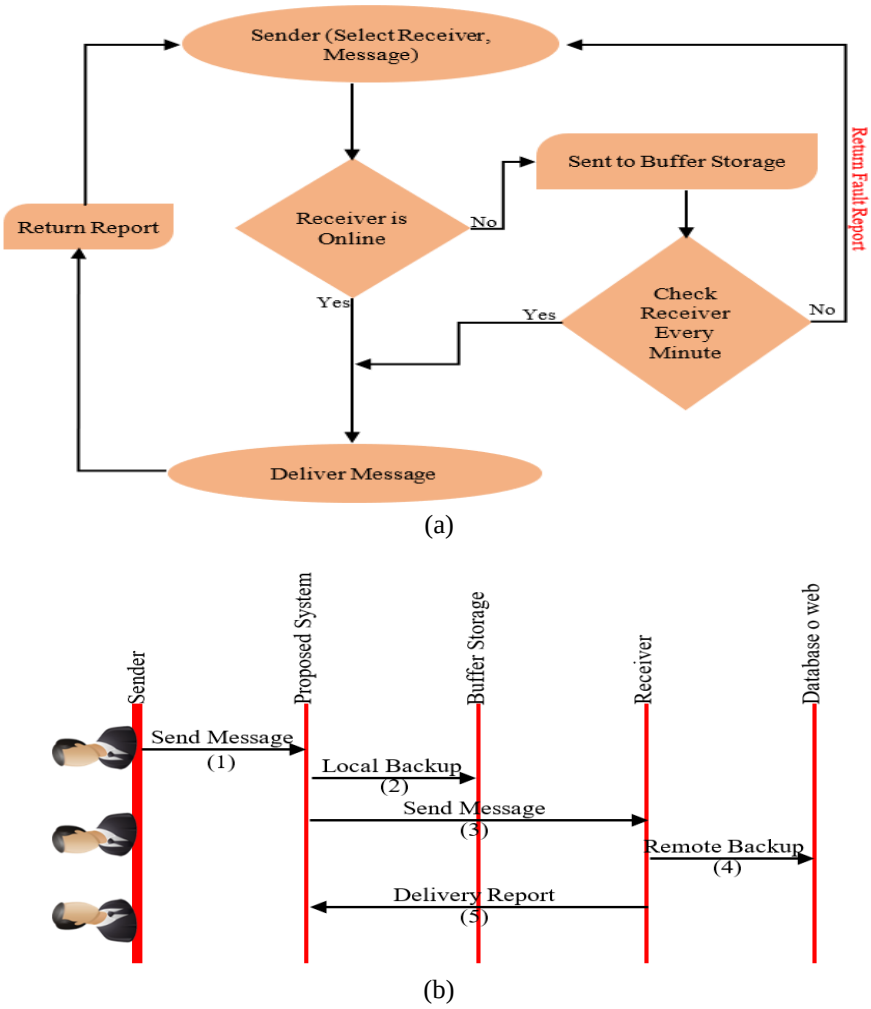


Figure 2. These figures are; (a) data movement between worker, (b) transactions of message exchange system

3.3. Database storage

A database has been created to organize several tables, the most important of which is a private table that stores public keys. The table includes a set of columns, the most important of which are the worker ID, the public key, and the date that that key was created. All workers within the system can see all public keys, names, and details of workers that are brought from another table based on the ID. The table of information workers includes the name, type car, number car, and the number of passengers for the car. Database tables are linked to the star schema. The database is located on the server web site for system administration. The database can be accessed through its path of the system's site provider.

3.4. Cryptography

3.4.1. Keys of encryption and decryption processes

The proposal relies on asymmetric cryptography to generate the keys used for encryption. The proposal is to use Elliptic curve to obtain these keys. The Elliptic curve is used to generate pair keys (public/private) without using to encrypt/decrypt the text. The pair keys generate from Elliptic curve are large digit numbers in each key. The public key is used for encryption by other users, while the private key is used by the same person to decrypted the sent text. The proposal generates the keys daily and automatically at (00:00:00) through the application designed with the smartphone. The key generation depends on a prime number (P) as this number is approved by all users within the system. The application is linked to the management system (trust anchor) which in turn grants a prime number for the keys to this day. The application sends the public key to the database for the system where all those who are associated with the company can view and use it. The proposal sends the public keys over an insecure channel. The Elliptic curve will depend on the equation:

$$y2 + axy + by = x3 + cx2 + dx + e \quad (1)$$

In the, (a-e) elliptic curves over the finite field are generally used and the discrete logarithm algorithm is realized by using the points of elliptic curves over the finite field to form finite groups. All coefficients are elements in the finite field GF (p). The proposal recommends the use of elliptic curve national institute of standards and technology (NIST) p192 [26] prime field having curve equation:

$$4a^3 + 27b^2 \, mod \, p \quad (2)$$

Where (a, b, and p) are predefined in Weierstrass elliptic form over a finite field (P). The elliptic curve has been used for faster computation. Depending on the value of (P) and the use of the elliptic curve equation, a point is chosen on the curve (G-the generator). The final parameters are n-the size of a subgroup-and h-the cofactor as point generation and straight slope calculation. On that, the key pairs are extracted. Through many different elliptic curve standards, curve 25519 (p256) was used. Base point G (X, Y) coordinates. The private key is saved to a temporary file inside the application for 24 hours only while the public key is not saved. The identification number for the worker, public key, and today's date is sent to the database on the Internet. The process of the elliptic curve is repeated every day to maintain the security of the handled pair keys between system workers.

3.4.2. Encryption data

In this proposal, the same key exchange algorithm was not used to encrypt and decrypt data. The elliptic curve algorithm is known for its speed and accuracy in making cryptographic keys. The RSA algorithm is more accurate in validation cryptography. Besides, the merging process increases the complexity of the attackers for the proposed system. To conduct the encryption process, it will take place at one of the parties of the system (the worker) who wants to send the message to administer the system or to anyone within the system. On this device, the prime number will have the initial from the system for today. It is also possible to display the names of the workers, from which the public key can be accessed by linking the tables via the identification number. The application requests specifying the receiving party (one or more workers) firstly, and then it writes the text of the message. To make it done, many procedures are taken:

- Fetching public keys (e) for recipient people.
- Initializing the prime number supplied by the company.
- Converting the text of the message to numbers through the american standard code for information interchange (ASCII) code table.
- Fragmenting the content of the message into blocks is less than the prime number and must belong to GF(p).
- Encrypting each block separately (End block maybe need padding if necessary) by using the encryption equation and the public key for each recipient.
- Converting the numbers to the text message through the ASCII code table.
- Combining ciphertexts with a single message and prepare for transmission.

The encryption process within the RSA algorithm is based on the following formula:

$$c = m^e \, mod \, p \quad (3)$$

Where c is the ciphertext, m is the message to block (e) the public key, and p is the prime number. The proposed system management cuts communication between workers at the last minute of each day to avoid sending messages using the keys of the previous day. The decryption process is based on speed and accuracy as the algorithms used are quick to implement and they are accurate in performance.

4. RESULTS

The proposed system relies on three main components (data, transmission over the web, and encryption). There is knowledge of the results of each one separately. The metrics within each component differ in how the results are calculated and how they are produced. The results were calculated from the proposed system after actually being applied experimentally for two months. The proposal employed 50 workers spread over nine spaced areas. Below, are the results calculated from the proposal:

4.1. The amount of data traffic transferred

In the early days, some workers face difficulty in dealing with the proposed system. Nevertheless, it recorded good results for the stored data traffic that circulated among workers. Figure 3 (a) and 3 (b) are the

data movement recorded on the first day of its implementation and the thirtieth day, according to the locations. So, Figures 4 (a) and 4 (b) represent data traffic for workers and the same days.

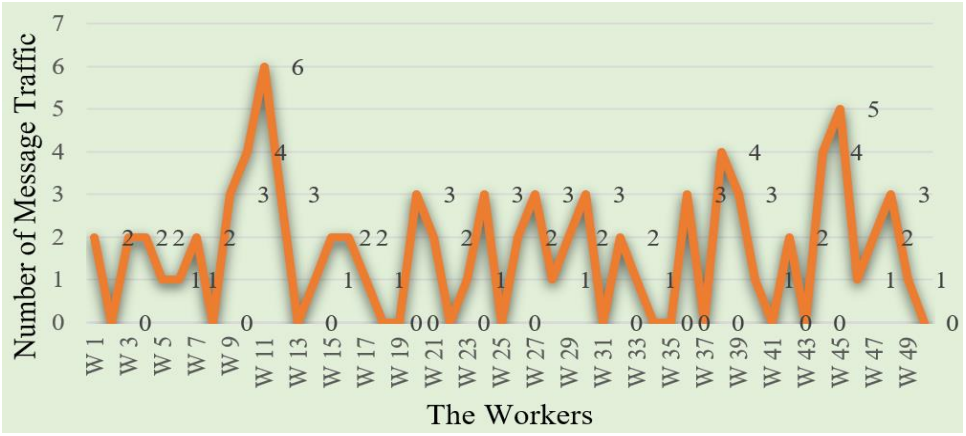
(a)

(b)

Figure 3. These figures are; (a) data traffic by location for the first day, (b) data traffic by location for the 30th day

(a)

Figure 4. These figures are; (a) data traffic by workers for the first day



(b)

Figure 4. These figures are; (b) data traffic by workers for the 30th day (*continue*)

From Figure (4), it appears that the traffic of the exchanged data within the system is uneven. The number of messages exchanged was weak in the first days of the application of the system. Data traffic stabilized in the second week to start the proposed system. It is noted that the amount of data traffic varies between workers, and this is due to the movement of workers from one location to another in which the number of customers varies. Data traffic also increases at the beginning of the week more than one and a half times of its traffic at the end of the week. Data traffic causes it to inflate over time, which is later required to analyze and extract knowledge. Table 1 shows data traffic by relying on locations of each week, and for a period of two months.

Table 1. Data traffic by locations for the 8th weeks

Locations	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
Loc 1	381	473	481	476	487	458	438	517
Loc 2	353	488	528	510	504	512	481	525
Loc 3	366	538	570	593	587	588	597	574
Loc 4	350	492	499	522	513	478	526	520
Loc 5	365	563	576	585	594	593	591	589
Loc 6	377	534	589	577	576	578	578	583
Loc 7	367	450	517	505	536	496	523	495
Loc 8	352	503	520	539	514	528	571	474
Loc 9	371	558	592	587	593	594	590	589

4.2. Data traffic cost for mobile app

The Internet is used to transfer data between workers through the mobile application. The network that workers use provides a good data transfer speed of 3.9 generations. The speed of the data transferred between the worker and the database varies from one receiving location to another. As the speed of data transmission depends on the strength of the Internet and the amount of data transferred in each transmission. The data transmitted with a minimum limit is 500 bytes (1/2 KB) and with a maximum limit (10 KB). Table 2. shows the data transmission speed encryption according to the proposed system and database. The time taken to transfer the same amount of data was not encrypted (original text). The difference was not much but it was faster than the encrypted text.

Table 2. Time of data traffic cost (original and encrypted data)

Data Block	Time (ms) for Original Data	Time (ms) for Encryption Data
0.5 KB	0.025	0.03
1 KB	0.078	0.09
3 KB	0.369	0.405
5KB	0.686	0.72
7 KB	0.852	0.935
10 KB	0.921	1.007

Messages are delivered between workers according to the proposed approach when they are in direct or indirect contact. In the case of direct communication, the encrypted data sent from the first worker to the second worker takes sufficient time to ensure that the second party receives them. Therefore, the time taken to exchange encrypted data between workers connected was calculated according to Table 3. In the case of indirect communication, the time taken to send the encrypted message to the buffering table is very close to the time taken to send the same data to the main database.

Table 3. Time of data traffic cost (direct and indirect connection between workers)

Data Block	Time (ms) of Direct Connection	Time (ms) of Indirect Connection
0.5 KB	0.033	0.031
1 KB	0.0928	0.091
3 KB	0.481	0.413
5KB	0.785	0.728
7 KB	0.991	0.949
10 KB	1.107	1.012

4.3. Encryption speeding time

4.3.1. Generate keys

In the proposal, the elliptic curve was used to generate the keys based on the prime number given by the administration. The proposed approach takes record time for the elliptic curve to generate the key pair (public and private). Key generation times are approximate depending on the length of the prime number. The prime numbers maybe 19 digits or 24 digits. This process takes place in the mobile application, which depends on the speed of implementing operations on the speed of the device. The operations were carried out on a group of devices with varying speeds and their results were very close. Table 4 shows the time taken to generate these keys.

Table 4. Execution time for key generation

Digits in Prime Number	Time in Millisecond
19	807
20	1036
21	1503
22	1348
23	1869
24	2339

4.3.2. Encryption and decryption process

To know the speed of the encryption and decryption of a specific text, the texts and keys must be equal. The keys generated are equal between all parties due to their dependence on one prime number. As for the messages, the same number of texts used to measure the amount of data transferred was encrypted. The process of encryption and decryption takes place inside smartphones, whose speed varies from one device to another. The time measurement was very close to the devices used. The encryption process takes more time than the decryption process and may reach weakness. This is due to two reasons, the first of which is that the encryption process calls for the recipient's public key from the database in the web and the second reason is that the decryption process is a mirrored process of encryption and it is repeated for all texts used. Also, the decrypted key is available on the same device.

5. CONCLUSION AND FUTURE WORK

In this paper, a system is designed to manage the interpersonal transport company. The management system is designed in a form that can be worked on from an office calculator that generates initial numbers every day. Employees generate the public key and the private key based on the initial number. The keys are generated via the Elliptic curve algorithm, which is considered one of the fastest in performing this algorithm. The data exchanged between the parties is encrypted using the RSA algorithm. Workers rely on their smartphones to exchange data through applications designed for the intended purpose. A database has been adopted across the web to store and facilitate data transferred between the parties. The system provides the management of companies and workers with services to manage them smoothly. As future work, IQ algorithms can be used to redeploy workers in most mobile cities between people. The system is also expected to be implemented in money transfer companies as it contains confidentiality in the transmission of information.

REFERENCES

[1] T. Guarda, M. F. Augusto, I. Lopes, J. A. Victor, Á. Rocha, and L. Molina, "Mobile Communication Systems: Evolution and Security," *Developments and Advances in Defense and Security MICRADS 2019*, Springer, Singapore, vol. 152, pp. 119-132, 2020, doi: 10.1007/978-981-13-9155-2_8.

[2] D. Nehra, K. S. Dhindsa, and B. Bhushan, "A Security Model to Make Communication Secure in Cluster-Based MANETs," *Advances in Intelligent Systems and Computing*, vol. 1079. pp. 183-193, 2020, doi: 10.1007/978-981-15-1097-7_16.

[3] N. Biswas, S. Chattopadhyay, and G. Mahapatra, "Computational Intelligence, Communications, and Business Analytics," vol. 775, pp. 242-255, 2017.

[4] F. M. Jasim, A. M. Sagheer, and A. M. Awad, "Enhancement of digital signature algorithm in bitcoin wallet," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 449-457, February 2021, doi: 10.11591/eei.v10i1.2339.

[5] D. K. Sarmah, A. J. Kulkarni, and A. Abraham, "Optimization Models in Steganography Using Metaheuristics," *Springer International Publishing*, 2020.

[6] J. R. Vacca, "Computer and Information Security Handbook," *Newnes*, 2012.

[7] O. A. Hammood, *et al.*, "An effective transmit packet coding with trust-based relay nodes in VANETs," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 685-697, April 2020, doi: 10.11591/eei.v9i2.1653.

[8] M. M. Faheem, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. Mat Deris, "A Survey on the Cryptographic Encryption Algorithms," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 11, pp. 333-344, 2017.

[9] O. A. Dawood, A. M. S. Rahma, and A. M. J. Abdul Hossen, "New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher," *International Journal Computer Network and Information Security*, vol. 9, no. 4, pp. 29-36, April 2017, doi: 10.5815/ijcnis.2017.04.04.

[10] W. Stallings, Computer Security: Principles and Practice, *Global Edition*. England, 2017.

[11] Z. Hercigonja, "Comparative Analysis of Cryptographic Algorithms," *International Journal of Digital Technology & Economy*, vol. 1, no. 2, pp. 127-134, 2016.

[12] A. Jha and S. Sharma, "Quantitative Interpretation of Cryptographic Algorithms," *Advances in Intelligent Systems and Computing*, Springer, Singapore, vol. 937. pp. 459-469, 2020, doi: 10.1007/978-981-13-7403-6_41.

[13] M. N. Dhivya and M. S. Banupriya, "Network Security with Cryptography and Steganography," *International Journal of Engineering Research & Technology (IJERT)*, vol. 8, no. 3, pp. 1-4, 2020.

[14] M. A. Mohammed and F. S. Abed, "A symmetric-based framework for securing cloud data at rest," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 28, no. 1, pp. 347-361, 2020, doi: 10.3906/elk-1902-114.

[15] Y. Yan, H. Xiaohong, and W. Wanjun, "Location-Based Services and Privacy Protection under Mobile Cloud Computing," *Bulletin of Electrical Engineering and Informatics*, vol. 4, no. 4, pp. 345-354, December 2015, doi: 10.11591/eei.v4i4.548.

[16] I. Eaton and M. McNett, "Protecting the data: Security and privacy," in *Data for Nurses*, 2020, pp. 87-99, doi: 10.1016/B978-0-12-816543-0.00006-6.

[17] M. Pant, T. K. Sharma, S. Basterrech, and C. Banerjee, "Performance Management of Integrated Systems and its Applications in Software Engineering," *Springer*, Singapore, 2020.

[18] A. Bhowmik, S. Karforma, and J. Dey, "Recurrence relation and DNA sequence: A state-of-art technique for secret sharing," *International Journal of Reconfigurable and Embedded Systems (IJRES)*, vol. 10, no. 1, pp. 65-76, March 2021, doi: 10.11591/ijres.v10.i1.pp65-76.

[19] H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou, "Flexible attribute-based proxy re-encryption for efficient data sharing," *Information Sciences*, vol. 511, pp. 94-113, February 2020, doi: 10.1016/j.ins.2019.09.052.

[20] S. A. Hameed, A. Haddad, M. H. Habaebi, and A. Nirabi, "Dermatological diagnosis by mobile application," *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 3, pp. 847-854, 2019, doi: 10.11591/eei.v8i3.150.

[21] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9110-9121, Sept. 2019, doi: 10.1109/TVT.2019.2927533.

[22] R. Kushwah, A. Kulshreshtha, K. Singh, and S. Sharma, "ECDSA for Data Origin Authentication and Vehicle Security in VANET," *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 2019, pp. 1-5, doi: 10.1109/IC3.2019.8844912.

[23] P. V. Jitha and U. S. Kumar, "Sms Security System Using Encryption Techniques," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 5, pp. 132-142, 2019.

[24] H. Y. Lin, M. Hsieh, and K. Li, "The Secure Vehicle-to-Vehicle and Vehicle-to-Group Communication Mechanisms in Smart City," *2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)*, 2018, pp. 186-192, doi: 10.1109/BigDataService.2018.00035.

[25] D. R. Prathama, P. A. W. Putro, and D. I. Naviangga, "Secure Mobile Payment Based on Elliptic Curve Cryptography," *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2018, pp. 140-145, doi: 10.1109/ISRITI.2018.8864488.

[26] W. Stallings, "Cryptography and Network Security: Principles and Practice," *Pearson Education*, India 2006.