IMPACT OF ADOPTION OF HOMOMORPHIC ENCRYPTION: SECURITY ENHANCE GUIDELINE FOR SRI LANKAN MILITARY SYSTEM

[1]RMKDLB Abeykoon, RT Udara, GAD Ganepola, WAAM Fernando, RPS Kathriarachchi, and DU Vidanagama

Department of Information Technology, General Sir John Kotelawala Defense University, Sri Lanka

[1]33-its-029@kdu.ac.lk

Abstract- At present, Information security increases the conversation with the occurrences of many data vulnerabilities in current systems. It is now mandatory for all system domains to consider and implement Information security plans. One current procedure which follows for securing information is Data Encryption, especially during end-to-end transmission across computer networks. Encryption is a method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Data Encryption has been and still is an area that is continuously being developed. As of today, the latest technology in this area is Homomorphic Encryption - conversion of data into ciphertext that can be analysed and worked with as if it were still in its original form. Ciphertext is plain text exposed to "Cipher" algorithm which is applied to plain text to get ciphertext. The authors present here the applicability of this technology on Sri Lankan Military Domain. The methodology used to conduct this research is a qualitative and quantitative based survey. The online survey was circulated through e-mail and the survey was successfully completed. According to the survey it could be analysed that the security when transferring data/information in this domain is very low-grade, which in contrast, must be very high due to the presence of sensitive data related to national security of the country. The authors have designed in detail on a set of recommended guidelines for secure transmission of military data using this technology.

Keywords- Information Security, Homomorphic encryption, Encryption Technology, Adoption of encryption.

I. INTRODUCTION

In computing, Encryption is the methodology by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if, they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks. There exist many modern and emerging technologies of Encryption such as Searchable Encryption, Homomorphic Encryption, Functional Encryption, etc.

Homomorphic Encryption in simple definition is, conversion of data into an encrypted format (i.e. ciphertext) and allows operations, functions, etc. to be performed on that format without the use of decrypting. Considering a real-world scenario, very important documents are kept inside a safe. However, it has to be taken out to perform any work in the documents. This creates a vulnerability of a certain data breach to occur. The above vulnerability can be discarded if work in documents can be done inside the safe. Homomorphic Encryption follows the exact scenario above. This technology allows complex mathematical operations to be performed on encrypted data without compromising the encryption. For instance, imagine two numbers that are not encrypted: 30 and 50. Once encrypted, the numbers become 43 and 72. The sum of the two encrypted numbers results in 115 (43 + 72). In homomorphic Encryption decryption of 115 the results in 80 (which is equivalent to the sum of the original numbers, 30 + 50).

The above technology of Encryption is used in many application domains where there is a high requirement of complex mathematical calculations which needs to be performed under high security for instance, high-end calculations in space stations, nuclear power plants, military operations, Bit coin mining, etc. In fact, Homomorphic encryption is an advantageous technology to avoid/minimize data breeches when data is being processed. This yet-developing technology attracts many researches to be performed. In this research paper, the authors researched on the application of Homomorphic Encryption into the operations of Sri Lankan Military. They have conducted a detailed requirement analysis by interviewing various personnel of the tri-forces and have recommended a guideline of methods of the application of Homomorphic Encryption.

II. OBJECTIVE OF STUDY

The authors scrutinize feasibility of applying homomorphic Sri Lankan Military domain with the aim of providing a higher data security during Military communication.

III. OVERVIEW OF METHODOLOGY

The authors formed a hypothesis which was tested by the responses gathered via an online survey. The authors then reviewed the responses and checked the correspondence between the responses and their hypothesis developed earlier in the process, thereby proposing a practical guideline of a real-time application.

The online survey was carried using a set of Military personnel in the Signal's unit of Sri Lankan Military domain.

IV. DATA ENCRYPTION: DEFINITION & PROCESS

Simply defining, Data Encryption is converting a message into another type of format so that the message meaning is not obvious.

To perform the encryption, it is essential for an encryption algorithm and an encryption key. The former being the mathematical calculation for the conversion and latter being the unique string of bits that determines the transformation through the algorithm.

The process of Encryption is as follows. Unencrypted data, plaintext, is encrypted using both the algorithm and the key. This process generates ciphertext that can only be viewed in its original form if decrypted with the correct key. Decryption is the reverse of encryption, the same steps but inversing the order in which the keys are applied.

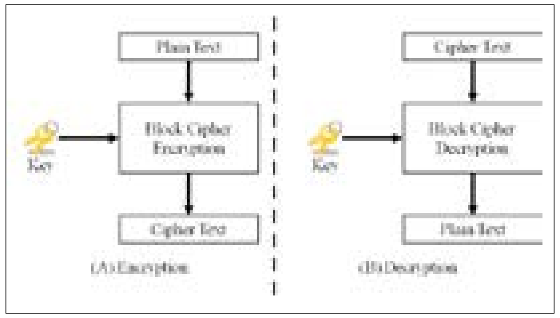


Figure 1. Diagram of encryption and decryption in Block Cipher
Source: Research Gate

Presently used encryption algorithms fall into two categories: Symmetric and Asymmetric Symmetric algorithm: Symmetric-key ciphers, also referred to as "secret key," use a single key. The most widely used symmetric-key cipher is the Advanced Encryption Standard (AES), which was designed to protect government classified information. Symmetric-key encryption is usually much faster than asymmetric encryption, however, the sender must exchange the key used to encrypt the data with the recipient before the recipient can perform decryption on the ciphertext. The need to securely distribute and manage large numbers of keys means most cryptographic processes use a symmetric algorithm to efficiently encrypt data but use an asymmetric algorithm to securely exchange the secret key.

Asymmetric algorithm: Asymmetric cryptography, also known as public key cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. The RSA encryption algorithm is the most widely used public key algorithm, partly because both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute provides a method of assuring not only confidentiality, but also the integrity, authenticity and non- reputability of electronic communication and data at rest using digital signatures.

V. HOMOMORPHIC ENCRYPTION: AN INTRODUCTION

Homomorphism as described in the research paper of Ogburn et al. "a mapping of a mathematical set into or onto another set or itself in such a way that the result obtained by applying those corresponding operations to elements of the first set is mapped onto the result obtained by applying those corresponding operations to their respective images in the second set."

The process of how this encryption methodology works has been explained clearly by Brian Hayes in American Scientist Journal via an article named "Alice and Bob in cipher space"

Consider two sets of data with one set, of positive real numbers, R, and the other, logarithms of real numbers. The multiplication of real numbers and the addition of logarithms are considered to be homomorphic operations. Considering x, y, z to be real numbers,

First operation: $x * y = z$

Second Operation: $\log(x) + \log(y) = \log(z)$.

There are two ways of obtaining the result z. First is to apply the operations to t plain text/unencrypted data and the second to encrypt the data (in this case takin the log values) apply a different operation to get a result and then converting the result to get the intended result. (taking the antilogarithm of z gives the result z).

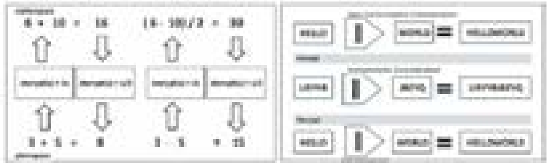


Figure 2. Encryption and decryption example
Source: American Scientist

V. COMPARISON OF HOMOMORPHIC ENCRYPTION WITH OTHER EXISITNG ENCRYPTION STRATEGIES

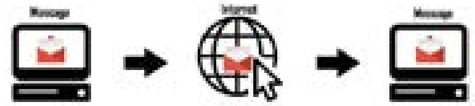


Figure 3. Basic message sending mechanism
Source: Author

Figure 3 depicts the traditional process of information transmission. Security and Encryption for any messages is unavailable which in turn allows any 3rd party to access and utilize the information.

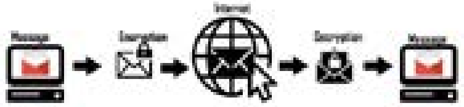


Figure 4. General message sending mechanism with data encryption
Source: Author

Figure 4 depicts the basic encryption strategy most parties use presently. The messages are encrypted into symbols and characters which are then transferred over the Internet or Intranet-work. However, anyone with the access to the decrypt key of the encryption strategy will be able to decrypt and access information.

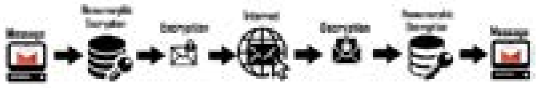


Figure 5. Message sending mechanism with homomorphic encryption
Source: Author

depicts the stages if the homomorphic strategy. Information is first homomorphically encrypted giving an output of with readable phrases but of complete irrelevance to original information's meaning. Next the homomorphic encrypted information is encrypted using normal strategies transforming to symbols and characters and transferred to the destination node via untrusted media.

The reason for encapsulating the homomorphic encrypted information using normal encryption strategies is to deceive the intruder that in case he captured the information and decrypted, he will be misled by the decrypted information because the decrypt information is provides meaningful phrases but is of complete irrelevance to original data

VI. IMPORTANCE OF DATA SECURITY IN MILITARY COMMUNICATION

Communication of data occurs through Wired Computer networks, Wireless networks or through physical means, that is man-to-man transmission. With the advancements of technology over the 21st Century, transmission of via physical means have reduced due to inefficiency & poor data security when compared to Wired/Wireless Computer networks. Data Security whilst transmitting through this mean is important due to the nature and quality of data being transmitted. Sri Lankan Military system uses an Intra-network and microwave based wireless technology for their communication. These networks constantly transfer to and from data that is vital for national defense of the country. It is mandatory that the data being transmitted need to be protect its confidentiality and kept out of reach of those any who are attempting to disrupt the nation's security. Hence, Information and Data Security acts as the "Heart of Military communication."

According to analysed data from online survey, the particular domain does not incorporate any such effective data encryption while performing data transmission. Since this system consist of highly confidential data related to national defence it is mandatory for potent data encryption strategy.

VII. APPLICATION OF HOMOMORPHIC ENCRYPTION TO SRI LANKAN MILITARY SYSTEM: A RECOMMENDATION

When compared to other Encryption technologies, this provides high end security for point-to-point transmission of military data. A scenario of the application would be, consider an important document regarding the current status of national security is sent from Defense Headquarters to a remote Military base. The document would be encrypted homomorphically. An algorithm would be conversion of letters in the document into another set of letters which would give another meaningful word but completely irrelevant to the originally transmitted document.

For instance, consider an original message from Colombo to Hambantota military base is sent. The message may include "Announcement to all Officers". When it is being transmitted over the intra-network it will be transmitted as "Roll Call Scheduled at 0800HRS". An intruder who intercepts the transmission media from middle are false guided by the homomorphic encrypted message. The intruder may be deceived of the transmitting messages as to not having encrypted, because the standard encryption implementations are producing ciphertexts which is a collection of letters, strings, symbols and tend to be encrypted.

Once the message reaches destination, it decrypts the data to the original message using homomorphic algorithms.

VIII. METHODOLOGY OF STUDY

A. Hypothesis

Based on Background Study, the authors developed a hypothesis which state that:

Homomorphic encryption is the optimum encryption strategy for the use of Military Communication due to the fact that:

a. During war & other crisis, military communication within their and among other teams play a key role. Locations, mission's statuses, war plans, daily objectives, etc. are some sensitive information being shared. Therefore, it is very much important to have a proper way to secure those messages when transferring from one place to another.

b. Current data encryption method or the mechanism Sri Lankan Military uses does not have a method to verify or retrieve all the messages on demand and it's a complex task to maintain a proper code (key) for every message. To send a message, a code is created particularly for the specific content and establish a connection across those two communication centers. At the receiving center, the location is confirmed message is retrieved using that specific code. Once the communication is over, the code that was used will not be used any longer, and a new code will be generated instead. But those messages are relatively very short messages which in turn makes it highly prone towards the risk of attackers and hackers.

c. With the introduction of homomorphic data encryption method, Sri Lankan Military can share their information about Locations, Mission's statuses, and other relatable information. Since this technology is yet under the development and in the terms of emerging technology, encryption is only possible for numerical information, such as locations, GPS status, and any other forms of communication which is done by numerical terms.

d. Main concern for the use of homomorphic encryption is because when the message is encrypted homomorphically, calculations can be performed while keeping the message in the encrypted state. Therefore, anything included in the message will not be decrypted, and hackers and attacker will not be encouraged to break such mechanisms very easily and read what was encrypted. Even if the calculations are done without decrypting. Final outcomes will be accurate and perfect. For an example if X=4, Y=5 and Z=1. when we decrypt it. Values of X, Y and Z will not be visible, but according to the homomorphic method we can still do calculations and get the accurate answer without decrypting those values.

e. Therefore, Homomorphic Encryption will be very much useful for Sri Lankan Military to share their information and statuses securely and in a most efficient way, and attacker or hackers will not be able to decrypt the message or read it.

B. Data Elicitation

The online survey was conducted with the intention of gathering responses to the following questions:

a. In the perspective of the militaria, Does Sri Lankan Military domain require to deploy any other encryption strategy apart from the current that is being used?

b. Does Sri Lankan Military domain be operationally feasible to adopt an emerging encryption strategy?

c. If, Homomorphic encryption was introduced as an emerging encryption strategy into the domain, would this be able to achieve the requirements of a secure military communication (in the context of militaria)

A group of interviewees of higher ranked officers in Sri Lankan Military Signals Unit were selected. The authors invited 120 personnel from which they received 100 responses. An online questionnaire series developed from Google Forms were sent to each personnel.

The authors selection behind the following interviewees is that:

The following questions were presented to the interviewees:

Q1. How is your knowledge on computer-based software and other IT related technical skills?

Q2. Are you aware that data security is now a prominent role in IT infrastructures?

Q3. In your opinion, do you consider that data security implemented at present meets with its current functionalities?

Q4. How would you recognize the reliability of the chain of command inside your organization?

Q5. Your opinion on the security of physical data transferring method (man-to-man)?

Q6. Your point of view on usefulness for updating of current data securing techniques?

Q7. Your opinion on your knowledge on data encryption?

IX. RESULTS & DISCUSSION

A. How is your knowledge on computer-based software and other IT related technical skills?

Majority of the Military personnel who were surveyed had an average knowledge on computer-based software programs and other IT skillset. As per the weights, the authors received an Average value of 80%, 10% of good and 7% 2% 1% on Very good, low and very low respectively from the Questionnaire being provided.

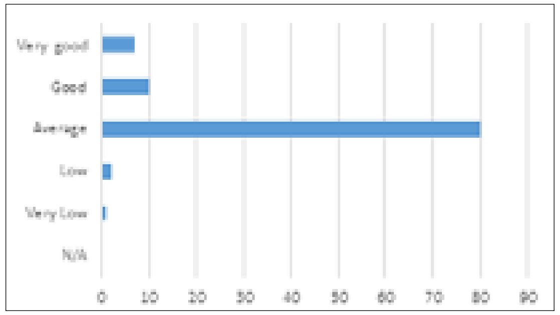
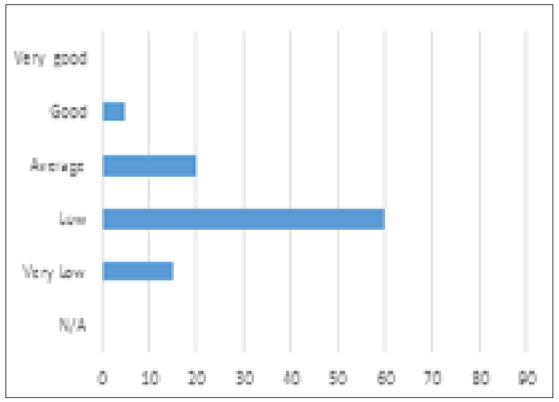


Figure 6. Analysed Data Chart
Source: Author

Based on the above figures, the authors observe that majority are proficient on the fast-changing Information Technology. With this base on mind, the authors drew a conclusion that majority personnel in the tri-forces would comprehend Homomorphic Data Encryption and accept & support for the implementation of this new technology in their domain system.

B. Are you aware that data security is now a prominent role in IT infrastructures?



Source: Author

The majority who answered this were those having sound knowledge on IT and working in the field related to IT. However, the weights showed a poor level on knowledge regarding data security. Weights were as follows 60% low, 20% average, 15% very low and 5% good. The authors were clear that there is a serious need of educating the personnel on importance of data security and enhance them with the value of Homomorphic data Encryption method.

C. In your opinion, do you consider that data security implemented at present meets with its current functionalities?

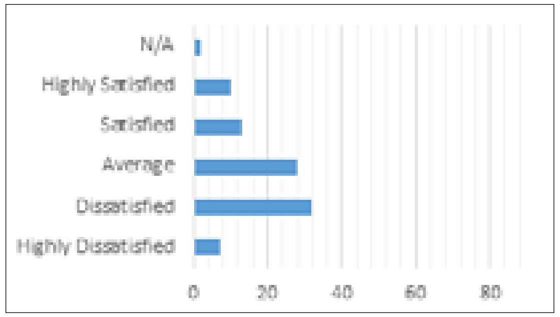


Figure 8. Analysed Data Chart
Source: Author

The authors revealed that wireless data transmission technology used currently is via microwaves. There is null deployment of data encryption technologies, which means Sri Lankan Military communicate over untrusted networks using plain texts.

Analysed data provide on the knowledge they have on their current data security and its functionalities, 32% of the personnel aren't happy with current data security functions and 28% of personnel are on a dilemma if the current data are well secured or not, therefore authors suggest data encryption and data security countermeasures must be applied in order to overcome vulnerabilities of current data security.

D. How would you recognize the reliability of the chain of command inside your organization?

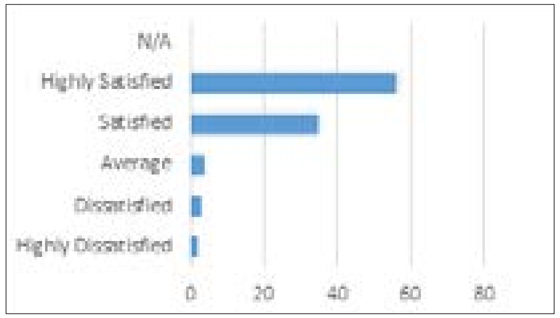


Figure 9. Analysed Data Chart
Source: Author

According to analysed data, 90% of personnel are on high recommendation of the reliability of their chain of command, therefore authors suggest the usage of homomorphically encrypted data inside the domain system as a method of securing data before any transmission occur for strictly permitting access for higher ranking officers.

E. Your opinion on the security of physical data transferring method (man-to-man)?

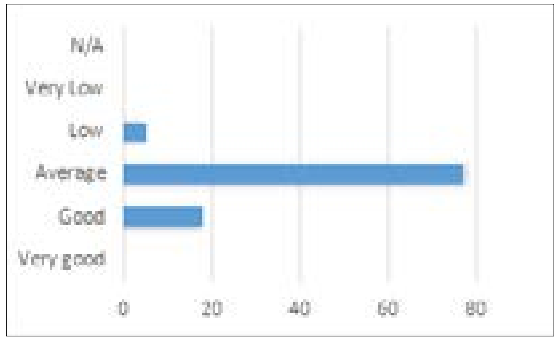


Figure 10. Analysed Data Chart
Source: Author

Most personnel consider that the security level is average in man-to-man data transferring technique. As shown in the results we got 77% of Average, 18% of good and 5% on low and 0% for the very low and very good from the survey. With the analyzation of these data authors concluded that there is an evident need of more secure method in physical data transferring.

F. Your point of view on usefulness for updating of current data securing techniques?

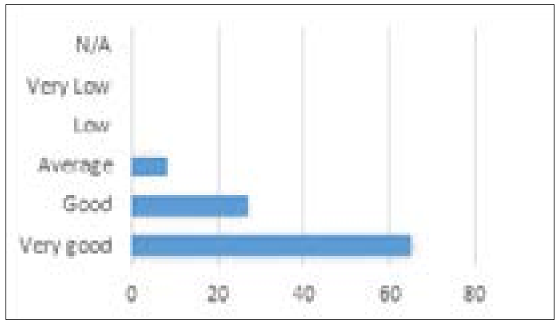


Figure 11. Analysed Data Chart
Source: Author

Majority's perspective was to use more updated data security techniques. As shown in the results weights obtained were got 65% of very good, 27% of good and 8% on Average and 0% for the low and very low. On analysation, authors concluded that there is an urge of more secure and updated method of data transferring such as Homomorphic data Encryption is required.

G. Your opinion on your knowledge on data encryption?

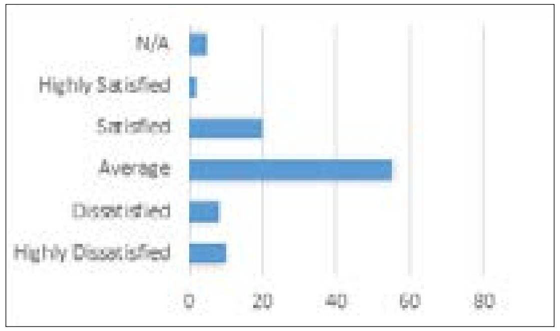


Figure 12. Analysed Data Chart
Source: Author

55% of the personnel who faced the survey are self-confident on their knowledge on data encryption. However, with consideration of every suggested guideline that is to be applied, they may have poor knowledge on data encryption and data security, based on as collected data, personnel are not familiar with data encryption and data security. Therefore, knowledge about data security and data encryption must be increased to update their data transmission techniques and current data security countermeasures.

X. CONCLUSION

Based on the above data gathered by the authors through online questionnaire, it is evident that majority of military personnel are aware of the theoretical background of Data security and its methodologies and its significance. However, practical implementation of Data Security strategies is not being implemented/ are being implemented but in very poor manner.

The authors came into an implication that it is a drive force that is required to integrate the domain system with the practical implementation of data security strategies. Hence, it is feasible to deploy an emerging encryption strategy like Homomorphic encryption in the domain.

Based on information gathered from military personnel, the authors' hypothesis was proven to be correct.

XI. FURTHER WORK

This paper introduces Homomorphic Encryption to Sri Lankan Military System to secure the Confidentiality, Integrity and Availability of data that is being communicated over transmission media. The authors have presented a recommendation of application of a Homomorphic encryption algorithm to minimize attacks.

Further works of this research include in developing a mathematically correct algorithm that would achieve the output of the designed algorithm, also can be discovered relationships and core relationships by doing this research more advanced using STSS software.

REFERENCES

B. Hayes, "Alice and Bob in cipherspace", American Scientist volume 100, 5,2012

Ogburn M., Turner C., Dahal P. , "Homomorphic Encryption", Procedia Computer Science(20), 502-509,2013

Pfleeger, C. and Pfleeger, S. (2012). Security in computing. Upper Saddle River: Prentice Hall.

Definition of Ciphertext | What Is Ciphertext ? Ciphertext Meaning. - The Economic Times. Accessed June 05, 2018. <https://economictimes.indiatimes.com/definition/ciphertext.>

Decrypting Data. - Accessed June 05, 2018. <https://msdn.microsoft.com/ja-jp/library/te15te69(v=vs.85).aspx.>

What Is Encryption? - Definition from WhatIs.Com. -SearchSecurity. Accessed June 07, 2018. <https://searchsecurity.techtarget.com/definition/encryption.>

Definition of Decryption | What Is Decryption ? Decryption Meaning. - The Economic Times. Accessed June 07, 2018. <https://economictimes.indiatimes.com/definition/decryption>