Available online at http://www.ijims.com

ISSN - (Print): 2519 – 7908 ; ISSN - (Electronic): 2348 – 0343

IF:4.335; Index Copernicus (IC) Value: 60.59; Peer-reviewed Journal

Cryptographic Chameleons: Adaptive Security Protocols for Dynamic Big Data Systems

Harish Janardhanan[1*]

[1*]Independent Researcher, 101 Mount Pleasant Ave, Edison, 08820, NJ, USA.

Abstract

It is important for security professionals to understand how safeguarding Big Data needs to adapt to the changing security thread which can be slow and inefficient with traditional approaches. The problem can be addressed by developing so called Cryptographic chameleons, which are security protocols that can adapt based on different aspects of data and security threats. This paper focuses on such protocols and evaluate the extent to which they provide protection to data integrity and confidentiality. This paper will be analyzing the typical approaches in the current literature and a new adaptive security concept suitable for the Big Data. The overall experimental results will show that the proposed solution will lead to faster and reliable improvements to security of the system.

Keywords: *Big Data, Adaptive Security, Cryptographic Chameleons, Data Integrity, Confidentiality*.

Introduction

In today's day and age, there is a massive influx of data which has affected the technological and business world in a rather profound way. This influx of data coming from different sources like Financial Transactions, Healthcare Records, IoT Sensors and Social Media Content is widely known as Big Data [1]. For a Big Data system, the general best practices using Traditional Security Protocols for securing the data relies on fixed Cryptographic keys and static security models, which cannot easily adapt to the changing phases of new threats prevalent in Big Data solutions, due to this an adaptive security protocol is a necessity to dynamically change the mechanisms of protection in response to the functioning of a system and its current levels of threats. These protocols use some of the modern features like dynamic key management, Context-Aware Encryption and real-time monitoring to secure Big Data systems. This paper discusses about an architectural design using the concept of Adaptive Security Protocol, specifically designed to integration with a Big Data System.

Literature Survey

Traditional Security Protocols

2.1.1 RSA (Rivest-Shamir-Adleman):

RSA is an algorithmic method which belongs to the class of public-key crypto systems for data exchange security. It is based on the question of how practically to solve the mathematical problem of factoring large prime numbers. RSA, which stands for Rivest, Shamir, and Adleman, is another encryption algorithm for encrypting data and the process of securing communications through the World Wide Web [5].

2.1.2 AES (Advanced Encryption Standard):

AES is known as a symmetric encryption algorithm standardized by the US government for protecting information. AES was designed by Joan Daemen and Vincent Rijmen, and due to its efficiency and security, it provides strong encryption using 128-, 192- or 256-bit keys [5].

2.1.3 SHA (Secure Hash Algorithm):

SHA has several hash functions used for solving graphic problems of data integrity assurance. SHA is an algorithm that was developed by the National Security Agency (NSA) in the United States; SHA always generates an output of a fixed size from input data to check its integrity. Some of the frequently used ones are SHA-1, SHA-256, and SHA-3 [7].

Limitations of Traditional Protocols

Even though, traditional security measures possess the qualities that are considered desirable in any field, there are certain drawbacks when using them. They depend on a set of parameters called Cryptographic keys, and these are static parameters, while the environments, the data structures and flows are not static. Usually, these protocols are used for stationary data

infrastructure, and because of this, they are not capable of handling real-time changes with the same proficiency, which exposes data to new threats [8]. Here are the limitations of traditional security protocols as also shown in the comparison in Tables 1:

2.2.1 Fixed Key Management:

Classic systems usually employ unchanging Cryptographic keys, also termed static keys; therefore, they are exposed to long-term key exposures and attacks [2].

2.2.2 Static Encryption Methods:

Traditional forms of encryption do not have the flexibility of dynamically adapting to the different types of data that may be passed through the network and the different levels of threat at different times; hence, they have limitations [2].

2.2.3 Inflexible Security Models:

Traditional security models do not adapt to today's fasting changing data structures [2] which is considered one of the main drawbacks of traditional security modles.

Adaptive Security in Cryptography

New ideas in the field of Cryptography developed recently are based on adaptive security. These mechanisms change the parameters of Cryptography based on the environment, providing better protection against new and emerging threats [9]. Here are the Examples of Adaptive Security and the comparison and limitations in Tables 2.

· *Dynamic Key Management Systems*: Based on the indicated system state and threat level, dynamic key management implies the re-generation of new keys periodically. This helps to eliminate opportunities for the exposure of keys and guarantees that keys are up-to-dated always [2, 10].

· *Context-Aware Encryption*: Context-based encryption modifies the degree of encryption together with algorithms with respect to circumstances under which data is accessed, retrieved or processed. This guarantees that sensitive data is protected with a maximum level of security that is proportional to its environment [3, 11].

Security Issues of Big Data

Peculiar to Big Data systems are the 4Vs: volume, variety, velocity, and veracity, all of which present novel security risks [1]. The amount of data multiplies the threats to the organization's digital perimeter; the types of data and the speed at which they are processed necessitate security adjustments in real-time to safeguard them efficiently [12].

· *Volume and Variety*: The nature of Big Data implies that enormous flows of highly sensitive data are always in the air. The nature of data, ranging from structured ones in databases to unstructured text data and media, demands different levels of protection [3].

· *Velocity and Veracity*: This implies that given the nature of data generation and processing speed, the requirement for security has to be constant. Completeness, the fourth dimension of big data quality, must also be upheld in order to avoid incongruence and erroneous analysis and decision-making [14].

Existing Adaptive Protocols

Several adaptive frameworks have been discussed in the literature, among which are the dynamic key management systems and the context-sensitive encryption techniques[15]. However, such protocols lack the flexibility to properly integrate with Big Data Systems.

Methods and Materials

Cryptographic Chameleons: System Architecture

System architecture proposal consist of various components containing dynamic key management, adaptive encryption module, and Real Time Monitoring (RTM) modules. All the above facets combine and process the security changes in accordance with the current state of the data system.

Figure 1 depicts the proposed approach for the deployment of the" Cryptographic Chameleons" to enable endogenous security for flexible and complex big data systems. The architecture comprises two primary components: the Big Data System and the Security Framework, these two components are composed of several modules connected to each other to allow an adequate management of data while preserving their security.

Starting with the user in the Big Data System, the process of creating data starts here. This is fed into the system through a data source. The raw data in the data ingestion module goes through a brief processing step. Subsequently. The data being processed is then stored in the data storage module when fully processed. One of the key objectives of this phase is to make data inaccessible by encryption to avoid being accessed by unauthorized persons; this way, data stored is safe.

In conjunction with the above operations, the security framework is active to improve the security of the data through constant observation and re-encryption based on current situations. Real time control sub-module is used for supervising the ingestion and processing steps that are applied to the input data. It supervises these procedures to identify deviations and, therefore, possible security risks. If such issues are detected, the real-time monitoring module calls a key update process, which is vital for security in a change-oriented environment.

The dynamic key management module comes into the picture to respond to these triggers by providing updated encryption keys. This mechanism makes it possible always to acquire up-to-date encryption keys that are applicable depending on the current security scenario. Following this, the context-aware encryption module employs the above dynamic keys to encrypt the said data. This encryption strategy makes the encryption scheme variable available to the conditions of data utilization hence enhancing security by making encryption respond to the current situation of use or threat.

Dynamic Key Management

Asymmetric key management entails the creation of fresh keys for encryption and decryption processes as well as the distribution of new keys to the desired parties and the revocation of old keys. These keys are created from current system parameters and data characteristics and are, as such, ever-changing. Dynamic key management comprises of the following as depicted in Figure 2.

1. *Monitor System Parameters:* The process starts with parameter surveillance, in this case, the ongoing observation of system parameters. This step helps to keep the current state of the system, including the performance level, security state, and metrics on how the system is performing constantly observed. Thus, by constantly monitoring the values of these inputs, the system will be able to recognize when adjustments to its Cryptographic demands may be required.
2. *Analyze Data Characteristics:* At the same time the features of data being processed by the system are also evaluated. Such considerations comprise the evaluation of various features of the data that is provided, such as the sensitivity of the data, the overall quantity of said data, and other characteristics that could be influencing the Cryptographic demands.
3. *Decision: Generate New Keys?* Depending on the monitored parameters and properties of the obtained data, an evaluation is made, and a decision is made on the generation of new Cryptographic keys. New keys must be created if the system conditions have changed and/or the features of the data necessitate it. This decision makes it possible always to ensure that the Cryptographic keys in use agree with the current security exigencies of the system.
4. *Generate Keys Based on Parameters (If yes):* If the decision is generating new keys, these keys are obtained from the present system configuration and data features. This step helps to make keys that fit into the given system requirements at a certain period. Adjusting keys to the current circumstances improves the protection and even the effectiveness of Cryptographic operations.
5. *Store Keys Securely:* After being produced, they are securely kept; the threshold between the two keys is then calculated; at this stage, a new key pair is generated. This step is important to ensure that the keys are not accessed or interfaced with by other parties, unlike what hackers intend to do. Encryption and storage of the keys in secure places like encrypted key vaults 16 are used to prevent attacks on the keys.
6. *Use Existing Keys (If not):* If the decision is not to generate new keys in the system, then reuse the old/used keys within the system. This implies that the current keys are considered reliable to meet the security requirement of the system from the current analysis. This is continued with existing keys to prevent the frequent generation of new keys; its preservers system was running.
7. *Distribute Keys to Authorized Entities:* Once keys have been generated and stored (or the decision is made to keep using other ones), they are immediately issued to the entitled parties. This step makes sure that only authorized bodies will be the ones to possess such Cryptographic keys needed for the secure transmitting of messages and data. Some of the measures that are taken to clear the misuse of the keys are strict observation of proper keying methods.
8. *Monitor Key Usage:* The system also actively watches how the keys are being utilized and this ensures to keep the consumers and investors informed with the latest developments happening around. This entails monitoring various attributes concerning key access and usage to identify improper behaviors. Monitoring on a continuous basis enables to keep the system's security intact and prevents unauthorized use of the keys.
9. *Decision: Revoke Keys?* From this monitoring, a decision is made whether yes certain keys shall be removed or not. This decision could be triggered by such factors as identifying that some keys are weak, or the keys are old or any discrepancy that is noted regarding the use of keys. A technique that revokes keys at the right time aims at avoiding threats of breaches as well as keeping the entire system assured.
10. *Revoke Compromised or Out-dated Keys (If yes):* Should the decision made be on revoking keys, then those keys that have been threatened or are no longer usable are revoked. This step is important so that there will be no alteration or modification to the Cryptographic system by third-party hackers. Revocation processes are performed without delay to eliminate any susceptibility towards the network as soon as possible.
11. *Continue Monitoring (If no):* If no key must be withdrawn, the system proceeds with the existing key. This makes it possible to have constant security watch and preparedness to respond if threats found again in the future.

Adaptive Encryption

One of the important parts of this architecture is the Adaptive encryption making it a Cryptographic Chameleon. Adaptive encryption changes the encryption algorithms and parameters in operations. This component currently assesses existing threats and system modifications and identifies the most suitable Cryptographic techniques to apply to data security and data integrity schemes.

Figure 3, depicted under the title Adaptive Encryption Process, presents a procedure to develop an approach for the adaptive change in Encryption Algorithms and Parameters looking against threats that emerged newly or based on system changes. This adaptive approach guarantees that the data will remain confidential and will be protected against any form of corruption in a real-time manner.

The concept entails starting from the assessment of the changes made to the system. This continuity assists in observing any changes or any new state of the system, which may affect its security status. In addition, there is a constant assessment of existing threats, too, of which the following are worthy of note. This entails a process of evaluating risks and searching for new or developing risks that are capable of jeopardizing information security.

With the information gathered from monitoring system changes and analyzing threats, a decision point is reached: The singular characteristic requiring its decision is whether the encryption algorithm should be tweaked or not. Should the decision be taken to shift the algorithm, the system identifies the proper Cryptographic type relevant to the present environment. It helps in having a perfect selection of the specific algorithm that would be suitable in combating the regarded threats and, at the same time, fit the changes being made in the system. Subsequently, there are changes in encryption parameters to ensure that the process of encryption is optimal, depending on the circumstances.

After choosing the encryption algorithm, the data is encrypted using the required algorithm together with the parameters set. This step helps to encrypt the data based on modern security measures and definite parameters.

Subsequently, to the encryption process, the overall effectiveness of the latter becomes tested and controlled. This entails determining whether the encryption technique is effectively safeguarding the records as well as if the data stays vulnerable to recognized risks.

If the encryption is effective, it remains watching both the process of encryption and the surrounding environment in order to be constantly vigilant. If this is the case, then the activities include re-evaluating threats and system modifications if the encryption is deemed to be ineffective. The helpful role of this reassessment is to figure out why there is a current failure of the encryption method and what change is needed.

According to these new assessments, the given algorithm and the parameters are subsequently revised. This step also ensures that the encryption method changes with the advancement in conditions in order to provide adequate security. In this case, a new algorithm, together with new parameters, is introduced, and the data is encrypted again and constantly supervised for efficiency.

This adaptive encryption can be descriptive of the necessity of a continuous and more conformal approach when it comes to data protection, analyzing the methods of encryption and comparing them with the threats and the changes in the system environment.

Results and Discussion

These are the expected results by assessment of the given framework in a Big Data setting that consisted of different data types, schema, amounts, and threats. The following are the expected performance in terms of data accuracy, security and breaches of data, time taken in encrypting/decrypting data and management of keys.

1. *Data Integrity and Confidentiality:* The use of adaptive security should display better results in data integrity and data confidentiality than the static security method. The context-based encryption should encrypt data depending based on the sensitivity of the data, in some instances more sensitive data will be given a lot more protection as compared to other data.
2. *Encryption/Decryption Times:* The ideal encryption algorithms, though a little more complicated will not influence the encryption/decryption times as the system can incorporate a Cryptographic accelerator. The dynamic key management system and the capacity to produce and distribute keys in real time will help reduce time to key generation and distribution.
3. *Key Management Efficiency:* Because of the dynamic key management process, the system will have the capacity to work with vast numbers of keys. One area in the proposed architecture that will ensure the highest degree of security is the fast removal and replacement of the keys that were impacted.

Case Study

This case study is to evaluate Cryptographic Chameleons architecture that is proposed in this paper by checking the feasibility of such a system specifically for system where data repositories are huge (Big Data). This architecture also needs to scale well without any performance degradation during dynamic key management.

For this case study we will have a parallel Cryptographic accelerator on a System on-Chip (SoC) to check the concept of Cryptographic Chameleons Framework on embedded systems. The primary objective is to secure the systems and defend the data transfers with respect to threats like bus monitoring, offline analysis, and data manipulation.

Key Features and Implementation

1. *Security Architecture:* In this architecture AES-Galois/Counter Mode (AES-GCM) Cryptographic acceleration is recommended to guarantee efficient and fast data processing and security during data transfer between the SoC and the main memory [17].
2. *Performance Evaluation:* The Cryptographic accelerator can be tested over a Xilinx Virtex-5 FPGA development board. The evaluation criteria to consider here is performance overhead, System Security.

Relevance to Cryptographic Chameleons Framework

· *Adaptive Security Protocols*: In this study, like the Cryptographic Chameleons, dynamic and context-aware encryption is adopted in the system by which the security mechanisms continue to adapt/update to new threats when they are encountered.

· *Dynamic Key Management:* The continuous updates to encryption key based on security threats will be notified to the system.

· *Scalability and Performance*: Frequent updates to security keys without considerable impact on the total performance can be achieved as research has shown when using AES-GCM [17].

Case study Results

These are the results expected

· *Performance Overhead:* The performance overhead of the Cryptographic accelerator will be relatively small based on how AES-Galois/Counter Mode works [18].

· *Security Assurance:* SoC will be quite efficient against data tampering attacks as we will be able to dynamically adapt to the threats by applying Adaptive Security Protocols paired with AES-CCM [18] accelerators to apply updates to encryption keys and mitigate the threats.

Conclusion

Deploying adaptive security protocols in non-static Big Data environments is valuable in ensuring organizational security in today's world which is characterized by big data proliferation. Data goes through many stages, including the collection stage, ingestion, processing, analysis, storage, and visualization and at every stage, it is vulnerable to several types of threats. Techniques of a Cryptographic nature, such as the use of encryption and access authorities, help protect data against break-ins and unauthorized access. Real-time threat analysis and constant protection make the system more secure by allowing organizations to respond to new threats as they evolve while also ensuring the safety and security of the data. Thus, including the security management concept that adapts to new threats, businesses will be able to prevent threats and maintain the confidentiality of these valuable assets.

Big Data systems are always evolving, and therefore, the security solution that is put in place needs to grow with it. Cryptographic chameleons, which are security protocols that can dynamically alter based on context and threats, give the best solution in today's world. Such protocols address data at rest and in transit, as well as help to improve the system's security against new types of threats.

References

[1] N. a. A. M. a. S. H. a. B. G. a. A. A. A. a. S. S. Khan, "The 10 Vs, Issues and Challenges of Big Data," *Association for Computing Machinery,* no. 18, p. 52–56, 2018.

[2] F. K. P. B. K. Y. W. K. B. K. Subhabrata Rana, "A comprehensive survey of Cryptography key management systems," *Journal of Information Security and Applications,* vol. 78, pp. 2214-2126, 2023.

[3] X. T. Xin Zhou, "Research and implementation of RSA algorithm for encryption and decryption," *International Forum on Strategic Technology, Harbin, Heilongjiang,* pp. 1118-1121, 2011.

[4] J. R. V. Daemen, "he Advanced Encryption Standard Process. In: The Design of Rijndael. Information Security and Cryptography," in *The Advanced Encryption Standard Process*, Berlin, Heidelberg, Springer, 2002, pp. 1-8.

[5] A. C. a. S. D. S. Debnath, "Brief review on journey of secured hash algorithms,," *International Conference on Opto-Electronics and Applied Optics ,* pp. 1-5, 2017.

[6] F. L. D. . Y. Long Cheng, "Enterprise data breach: causes, challenges, prevention, and future directions," *WIREs Data Mining Knowl Discov ,* 2017.

[7] R. C. H. K. Mihir Bellare, "Keying Hash Functions for Message Authentication," *Springer-Verlag,* p. 1–15, 1996.

[8] A. B. H. B. Sahar Ahmadi Khah, "A dynamic and multi-level key management method in wireless sensor networks (WSNs)," *Computer Networks,* vol. 236, pp. 1389-1286, 2023.

[9] E. &. A.-H. S. Al-Shaer, ”Flow-based Security Management for Large Scale Networks,” *Proceedings of the 26th Annual Computer Security Applications Conference,* pp. 69-78, 2010.

[10] E. V. Y. P. I. A. D. M. G. Psarra, ”A Context-Aware Security Model for a Combination of Attribute-Based Access Control and Attribute-Based Encryption in the Healthcare Domain,” *Advances in Intelligent Systems and Computing,* vol. 1150, p. 1133–1142, 2020.

[11] Z. T. H. R. K. &. H. Y. T. Zhou, ”Real-Time Context-Aware Encryption for Streaming Data in Healthcare Systems,” *IEEE Transactions on Information Forensics and Security,* pp. 1217-1231, 2015, 10(6).

[12] M. M. S. &. L. Y. Chen, ”Big Data: A Survey,” *Mobile Networks and Applications,* pp. 171-209, 2014, 19(2).

[13] A. &. H. M. Gandomi, ”Beyond the Hype: Big Data Concepts, Methods, and Analytics,” *International Journal of Information Management,* pp. 137-144, 2015,35(2).

[14] A. W. M. &. G. R. H. Katal, ”Big Data: Issues, Challenges, Tools and Good Practices,” *Sixth International Conference on Contemporary Computing (IC3),* pp. 404-409, 2013.

[15] Y. G. M. &. E.-K. K. Gahi, ”Big Data Analytics: Security and Privacy Challenges,” *IEEE Symposium on Computers and Communication (ISCC),* pp. 952-957, 2016.

[16] H. S. K. K. Poonam Yadav, ”Introducing real-time image encryption technology using key vault,” *springer,* vol. 82, p. 39099–39117, 2023.

[17] Z. Zhang, X. Wang, Q. Hao, D. Xu, J. Zhang, J. Liu and J. Ma, ”High-Efficiency Parallel Cryptographic Accelerator for Real-Time Guaranteeing Dynamic Data Security in Embedded Systems,” *Micromachines,* vol. 560, p. 12, 2021.

[18] L. M. W. M. H. J. Nabihah Ahmad, ”Advanced Encryption Standard with Galois Counter Mode using Field Programmable Gate Array,” *Journal of Physics,* 2018.

Tables and Figures

Table 1: Comparison of Traditional vs. Adaptive Security Protocols

Feature	Traditional Protocols	Adaptive Security Protocols
Key Management	Fixed	Dynamic
Encryption Methods	Static	Adaptive
Security Model	Inflexible	Flexible

Table 2: Comparison of Adaptive Security Protocols

Protocol	Description	Limitations
Dynamic Key Management	Periodic renewal of Cryptographic keys	Scalability issues with large data volumes
Context-Aware Encryption	Adjusts encryption based on data context	Slow adaptation to rapidly changing threats

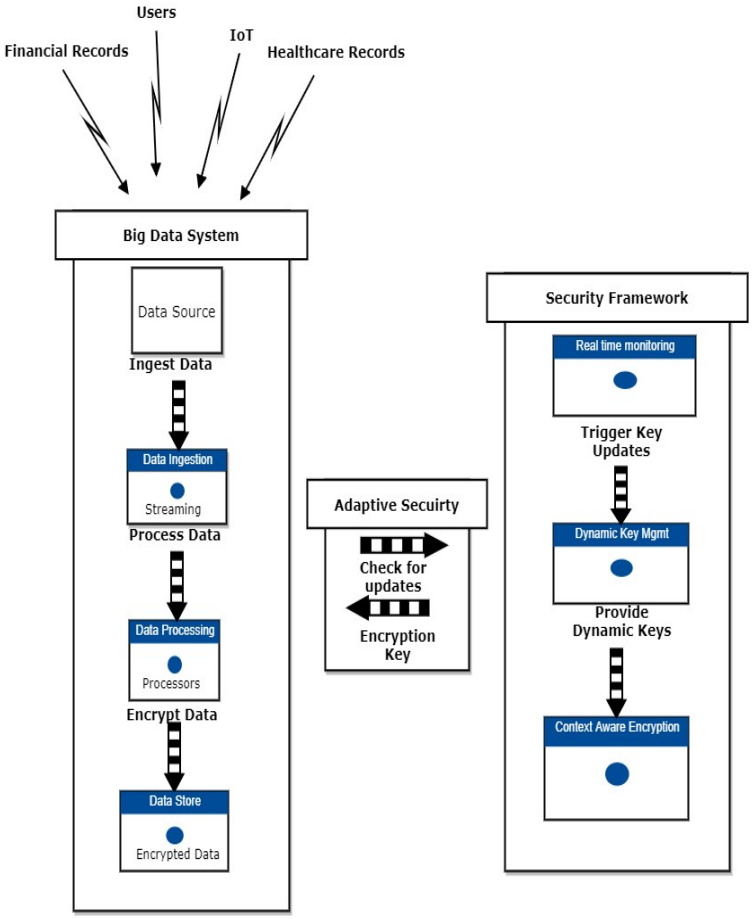

Fig. 1: System Architecture of Cryptographic Chameleons Framework

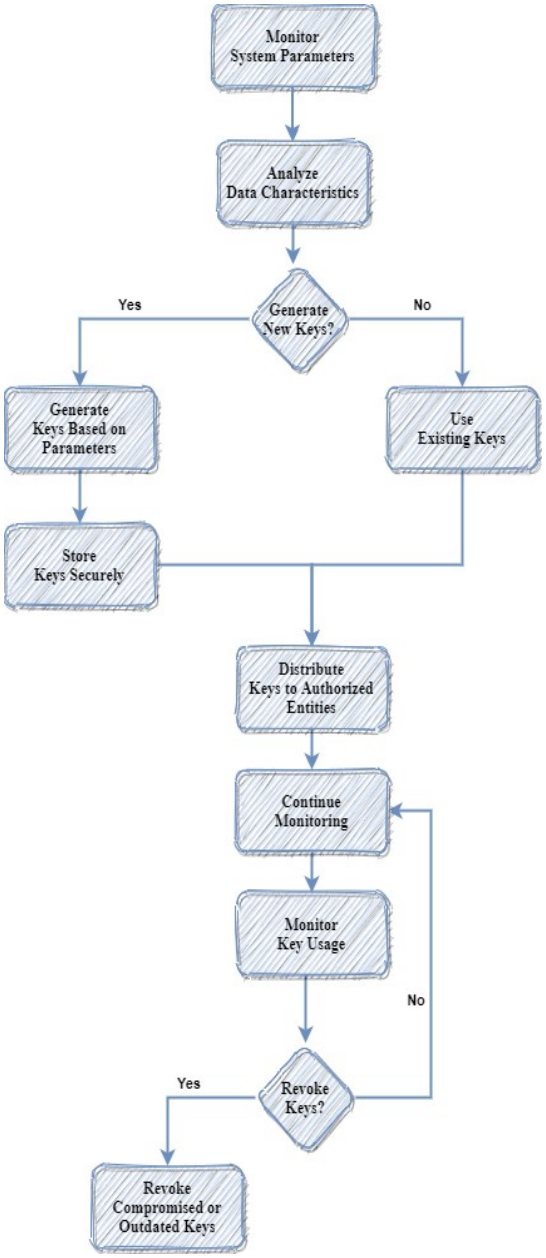

Fig. 2: Dynamic Key Management Process

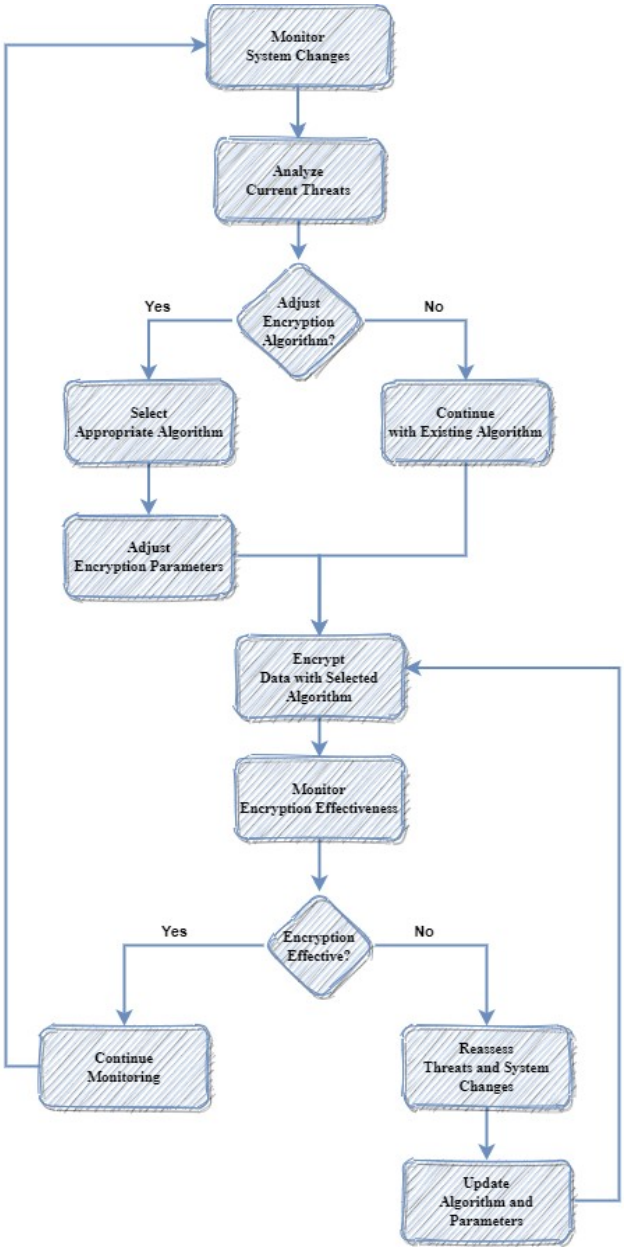

Fig. 3: Adaptive Encryption Process.