International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Effective Validation for Pervasive Computing and Mobile Computing Using MAC Algorithm

Atharv Arun Yenurkar [a], Asst Prof. Neehal B. Jiwane [b], Asst. Prof. Ashish B. Deharkar [c]

[a] *Shri Sai College of Engineering & Technology, Bhadrawati, Chandrapur 442902, India*
[b] *Shri Sai College of Engineering & Technology, Bhadrawati, Chandrapur 442902, India*
[c] *Shri Sai College of Engineering & Technology, Bhadrawati, Chandrapur 442902, India*

A B S T R A C T

At present many applications rely on the survival of small devices that can swap information and form communication networks. And it is tough to provide safety for such application. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest By using Advance Encryption algorithm we are authenticating the message which is encrypted and we are recovering the decryption speed and authentication correctness to protect the communication the proposed message authentication technique is more efficient than the previous message authentication algorithms and the aim of this proposed techniques is to use the safety that the encryption algorithm can provide to plan more useful authentication mechanisms, as opposed to using standalone authentication primitives. It provides the security to the data. Yet it has high risk to the sender input data while receive transmission data to receiver. The procedure will be evaluated in the real time situation in terms of the networking atmosphere. The routine will be examine in terms of the time complexity of the entire process.

Keywords: message authentication technique, encrypt-and-authenticate, pervasive computing, authentication.

1. Introduction

Preserving the reliability of messages replace over public channels is one of the classic aim in cryptography and the literature is rich with message authentication code algorithms that are designed for the only purpose of preserving message reliability. Conserving the honesty of messages traded over open channels is one of the excellent objectives in cryptography also the literature is rich with message authentication Code algorithm that are intended for the sole motivation behind Conserving message truthfulness. In light of their security, Macs can be either genuinely or computationally secure. Genuinely secure MACs give message authentication against counterfeiter with boundless computational force. On the other hand, computationally secure MACs are just secure at the point when counterfeiters have restricted computational force..We can use the universal hash-function families to the design of unconditionally secure authentication as these are not restricted. Automatically protected MACs relay on universal hash functions can be developed with couple of rounds of computations. In the initial round, the message which we are authenticating is squashed using a universal hash function. Then, in the later round, the squashed image is developed with a cryptographic function (typically a pseudorandom function1). Popular automatically protected universal hashing-based MACs include, but are not inadequate.

In another application, consider the increasingly spreading deployment of radio frequency identification (RFID) systems. In such systems, RFID tags need to identify themselves to authorized RFID readers in an authenticated way that also preserves their privacy. In such scenarios, RFID tags usually encrypt their identity, which is typically a short string (for example, tags unique identifiers are 64-bit long in the EPC Class-1 Generation-2 standard), to protect their privacy. Since the RFID reader must also authenticate the identity of the RFID tag, RFID tags must be equipped with a message authentication mechanism . In this paper our contribution is Literature survey, our proposed method, architecture diagram and advantages also conclusion and future scope.

2. Literature Survey

In this paper, proposed universal hash functions that has been appeared repeatedly in the literature and provide a detailed algebraic analysis for the security of authentication codes based on this universal hash family. No earlier work has studied the extension of such universal hash family when computations are execute module a non-prime integer n. In this work, they give the first such analysis. They examine the safety of authentication when computations are performed over arbitrary finite integer rings Zn and derive an explicit relation between the prime factorization of n and the bound on the probability of successful forgery. More specifically, they show that the probability of successful forgery against authentication codes based on such a universal hash-function family is bounded by the reciprocal of the smallest prime factor of the modulus n. In this paper, proposed a generic method of create such channels is by combining an encryption primal with an authentication primitive . In this work, they introduce the design of a new cryptographic primitive

to be used in the build of secure channels. Instead of using general purpose MACs, they propose the employment of special purpose MACs. The main aim behind this work is the examination that, the message must be both encrypted and authenticated, there can be a redundancy in the computations examine by the two primitives. If this turned out to be the case, removing such redundancy will get better the useful of the overall build. In addition, computations execute by the encryption algorithm can be further used to improve the security of the authentication algorithm. In this work, they illustrate how E-MACs can be designed to reduce the amount of computations required by standard MACs based on universal hash functions, and show how E-MACs can be secured against key-recovery attacks This paper shows that carefully coded implementations of these hash functions are able to exploit the Pentium's superscalar architecture to its more effect: the performance with respect to performed on a non-parallel **ar**chitecture improved by about 65%. This is an key result in view of the current claims on the limited data bandwidth of these hash functions. Also, it is conjectured that these operation are very close to optimal. It will also be shown that performance penalty incurred by non-cached data and conversion is limited, and in the order of 15% of running time

3. Problem Statement

Currently, many applications depend on the existence of small devices that can swap information and form communication networks. And it is very difficult to provide security for such application. At the same time, the confidentiality and integrity of the communicated messages are of particular interest. Therefore we suggest an application which boosts the security of the application. We suggested an algorithm which boosts the security and performance of the message authentication technique.

4. Proposed System

We suggest the following research problems: if there is an application in which messages that need to be swap are short and both their isolation and reliability need to be protected, can one do better than simply encrypting the messages using an encryption algorithm and validate them using standard message authentication technique? We answer the problem by proposing two new techniques for authenticating short encrypted messages that are more efficient than existing approaches. In the first technique, we develop the fact that the message to be authenticated is also encrypted, with any secure encryption algorithm, to append a short casual string to be used in the authentication process. The below fig.1 shows the architecture of our proposed system.

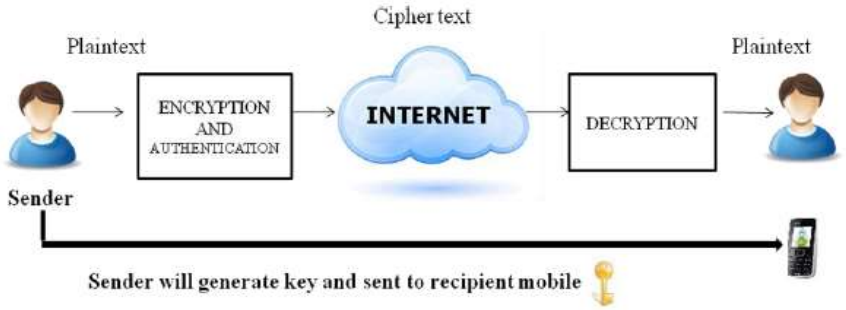

Fig.1 Architecture of proposed system

Implementation Modules

1. Authenticating Short Encrypted Messages

2. Security Model

3. Security of the authenticated encryption composition

4. Data privacy

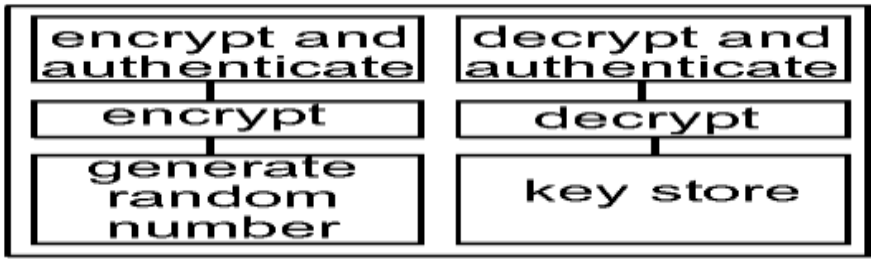

Fig 2. Message Authentication System

4. 1. Authenticating short encrypted messages

In this paper, we describe our first authentication scheme that can be used with any IND-CPA safety encryption algorithm .An key idea we make is that messages to be verified are no longer than a predefined length. This contain applications in which messages are of fixed length that is known a priori, such as radio frequency identification systems in which tags need to validated their identifiers, sensor nodes reporting events that belong to certain domain or measurements within a certain range, etc. The novelty of the suggested idea is to utilize the encryption algorithm to distribute a changes string and use it to reach the simplicity and useful of one-time pad validated without the need to handle impractically long keys.

4.2. Security Model:

A message valideted scheme consists of a signing algorithm S and a verifying algorithm V. The signing algorithm force be probabilistic, while the verifying one is usually not. Associated with the idea are parameters and N describing the length of the shared key and the resulting authentication tag.

4.3. Security of the Authenticated Encryption Composition:

In this module paper, it defined two ideas of integrity for valideted encryption systems: the first one is integrity of plaintext (INT-PTXT) and the second one is integrity of cipher text (INT-CTXT). Joined with encryption algorithms that gives in-distinguish ability under elected plaintext attacks (IND-CPA), the safety of different methods for makinging generic compositions are analyzed. Note that our structure is an occurrence of the Encrypt-and-Authenticate generic work since the plaintext message goes to the encryption algorithm as an input, and the same plaintext message goes to the valideted algorithm as an input.

4.4. Data Privacy:

Remember that two pieces of data are send out to the intended receiver (the cipher text and the authentication tag),both of which are task0s of the private plaintext message. Now, when it comes to the validation tag, observe that then once r serves as a one-time key (similar to the role r plays in the construction of Section. the formal study that the authentication tag does not compromise message privacy is the same as the one provided. The cipher text of equation, on the other hand, is a standard CBC encryption and its sefaty is well-learned; thus, we give the theorem report below without a formal.

Now day's reality, numerous applications depend on the attendance of little gadgets that can operate data and construct correspondence systems. In a critical segment of such applications, the retreat and respectability of the imparted messages are specifically compelling. The security and integrity to be maintained by the communication within the system required following methods.

1. Encryption methods.

2. Authentication methods.

3. Data and security analysis.

5. Results

In existing system developed the fact that the message to be validated is also encrypted, with any safety encryption algorithm, to append a short random string to be used in the validation process. Given that the random strings used for different processes are independent, the authentication algorithm can benefit from the simplicity of unconditional secure authentication to allow for faster and more efficient authentication. Use of encryption algorithm is block cipher based to further recover the computational efficiency of the technique. The driving motive behind study is that using a general purpose massage authentication algorithm to authenticate swap messages in such systems might not be the most useful solution and can lead to waste of resources already available, namely, the safety that is provided by the encryption algorithm.

In the suggested system we generate the random string and that random string is used as a key that will sent to the recipient directly to his personal mobile phone so that there should be integrity in the communicated messages, and encryption methods are the data encryption standard and the advanced encryption standard which includes the modular operations which are fast. For instance, while the cryptographic hash functions SHA-256 and SHA-512 run in about 23.73 cycles/byte and 40.18 cycles/byte, respectively, the modular multiplication runs in about 1.5 cycles/byte.

In suggested system we have less time complexity, less computational cost, effective integrity, more secure while the transmission, more confidential.

6. Conclusion

In this paper a new methodology for authenticating tiny encrypted messages is projected. The truth that the message which is to be authenticated must need to be encrypted is utilized to provide a arbitrary nonce to the proposed receiver via the cipher text. This permits the design of a validation code those profits from the simplicity of absolutely secure validation with no need to handle one-time keys.

Mainly, it has been confirmed in this paper that validation tags can be calculated with one calculation and a one modular multiplication. Assured that messages are comparatively short, addition and modular multiplication can be execute quicker than presented computationally secure MACs in the journalism of cryptography. When devices are equipped with block ciphers to encrypt messages, a second technique that utilizes the fact that block ciphers can be modeled as strong pseudorandom permutations is proposed to authenticate messages using a single modular addition. The suggested schemes are shown to be orders of magnitude faster, and consume orders of magnitude less energy than traditional MAC algorithms. Therefore, they are more appropriate to be used in computationally constrained mobile and pervasive devices.

7. Future Scope

In the future have to investigate about the further execution of encryption techniques to enhance the process with the fewer time complexity and the high integrity in the process. And have to improve the whole performance by implementing the other process oriented to the security of the data in the mobile computing process. And also need to investigate about the other possible ways to improving the data security other than the cryptographic techniques as the additional process to the data security of the data.

8. References

1. B. Alomair, A. Clark, and R. Poovendran, “The Power of Primes: Security of Authentication Based on a Universal hash-Function Family,” J. Math. Cryptology, vol. 4, No. 2, 2010.

2. A. Bosselaers, R. Govaerts, and J. Vandewalle, “Fast hashing on the Pentium,” in Advances in Cryptology-CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 298–312

3. Pratiksha S. Bodhe, Neehal B. Jiwane published paper in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) on the topic “ Design and Implementation of E-learning System” on Vol. 11, Issue 5, May 2022

4. B.Alomair and R. Poovendran, “Efficient Authentication for Mobile and Pervasive Computing,” Proc. 12th Int’l Conf. Information and Comm. Security (ICICS ’10), 2010.

5. Viraj Kalambe, Neehal B. Jiwane published paper in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) on the topic “ College Enterprises and Resources Planning” on Vol. 11, Issue 5, May 2022

6. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway,“UMAC: Fast and Secure Message Authentication,” Proc. 19th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’99), pp. 216-233, 1999.

7. Sujata Bhalme, Neehal B. Jiwane published paper in International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) on the topic “ Digital voting system using on blockchain” on Vol. 11, Issue 5, May 2022

8. T. Helleseth and T. Johansson, “Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings,” Proc. 16th Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO ’96), pp. 31-44, 1996.