International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Dynamic Verification for Mobile and Prevalent Computing

MR. AMIRISHETT RAJU [1] & MS. V. NIHARIKA [2]

[1]Assistant Professor Department of CSE Vaagdevi Engineering College, Bollikunta, Warangal, and Telangana State, India.

[2]M-Tech Computer Science & Engineering Department of CSE Vaagdevi Engineering College, Bollikunta, Warangal, and Telangana State, India.

Abstract: With today's technology, many packages depend on the lifestyles of small devices that could trade statistics and form communication networks. In a sizeable portion of such packages, the confidentiality and integrity of the communicated messages are of specific interest. In this work, we propose novel strategies for authenticating short encrypted messages which might be directed to satisfy the necessities of cellular and pervasive programs. by using taking advantage of the reality that the message to be authenticated ought to also be encrypted, we suggest provably comfy authentication codes which can be extra green than any message authentication code inside the literature. the important thing concept at the back of the proposed strategies is to make use of the security that the encryption set of rules can offer to layout extra efficient authentication mechanisms, in place of using standalone authentication primitives.

Index terms: Authentication, unconditional protection, computational safety, commonplace hash-function families, pervasive computing

1 CREATION AND ASSOCIATED WORKS

Retaining the integrity of messages exchanged over public channels is one of the classic desires in cryptography and the literature is rich with message authentication code (MAC) algorithms which might be designed for the only motive of maintaining message integrity. Primarily based on their protection, MACs may be both unconditional/ computationally comfy. Unconditionally cozy MACs offer message integrity in opposition to forgers with limitless computational power. at the different hand, computationally secure MACs are simplest secure when forgers have restricted computational electricity. A popular class of unconditionally comfy authentication is based totally on everyday hash-function families, pioneered by means of Carter and Wegman. On account that then, the examination of unconditionally comfortable message authentication based totally on conventional hash functions has been attracting research attention, each from the layout and analysis standpoints. The primary concept taking into account unconditional safety is that the authentication key can simplest be used to authenticate a limited quantity of exchanged messages. Since the control of one-time keys is taken into consideration impractical in lots of applications, computationally cozy MACs have become the method of preference for most actual-existence programs. In computationally comfortable

MACs, keys may be used to authenticate an arbitrary number of messages. That is, after agreeing on a key, valid customers can alternate an arbitrary quantity of authenticated messages with the equal key. Relying on the main constructing block used to assemble them, computationally relaxed MACs can be labeled into three essential classes: block cipher based, cryptographic hash feature based totally, or standard hash-function circle of relatives primarily based.

CBC-MAC is one of the maximum known block cipher-based MACs, exact inside the Federal facts Processing standards book 113 and the global enterprise for Standardization ISO/IEC 9797-1. CMAC, a modified version of CBC-MAC, is provided inside the NIST unique book 800-38B, which became primarily based on the OMAC. Other block cipher-based MACs encompass, however are not confined to, XOR-MAC and PMAC. The safety of various MACs has been exhaustively studied. The use of a one-way cryptographic hash capability for message authentication becomes added via Tsudik. A popular instance of the use of iterated cryptographic hash features within the design of message authentication codes is HMAC, which became proposed through Bellare et al. HMAC become later adopted as a general. Any other cryptographic hash feature-primarily based MAC is the MDx-MAC proposed by using Preneel and Van Oorschot. HMAC and two editions of MDx-MAC are certain in the global corporation for Standardization. Bosselaers et al. defined how cryptographic hash features may be carefully coded to take benefit of the shape of the Pentium processor to speed up the authentication method. Using commonplace hash-characteristic families inside the Carter-Wegman fashion isn't restricted to the layout of unconditionally cozy authentication. Computationally secure MACs based on regular hash features can be constructed with two rounds of computations. Within the first round, the message to be authenticated is compressed using a general hash feature. Then, within the 2d round, the compressed picture is processed with a cryptographic characteristic (generally a pseudorandom function1). Indeed, general hashing-based totally MACs give better performance whilst as compared to dam cipher or cryptographic hashing-based MACs. In reality, the fastest MACs in the cryptographic literature are based totally on common hashing. The primary cause at the back of the performance benefit of everyday hashing-based MACs is the reality that processing messages block by block the use of universal hash functions is orders of significance quicker than processing them block by way of block the usage of block ciphers or cryptographic hash functions. One of the primary differences between unconditionally at ease MACs based on universal hashing and computationally cozy MACs primarily based on common hashing is the requirement to technique the compressed picture with a cryptographic primitive inside the latter magnificence of MACs. This round of computation is essential to guard the name of the game key of the standard hash feature. that is, due to the fact familiar hash capabilities aren't cryptographic functions, the remark of more than one message-photograph pairs can reveal the value of the hashing key. Because the hashing secret is used repeatedly in computationally comfy MACs, the publicity of the hashing key will lead to breaking the safety of the MAC. Accordingly, processing the compressed photo with a cryptographic primitive is necessary for the security of this elegance of MACs. This implies that unconditionally comfortable MACs primarily based on commonplace hashing are extra efficient than computationally comfortable ones. on the poor aspect, unconditionally secure standard hashing-

based totally MACs are taken into consideration impractical in maximum modern-day packages, due to the issue of coping with one-time keys.

There had been huge efforts devoted to the design of hardware green implementations that suite such small gadgets. for example, hardware efficient implementations of block ciphers have been proposed in. Implementations of hardware green cryptographic hash functions have also been proposed. But, there was very little effort in the design of special algorithms that may be used for the layout of message authentication codes which could utilize different operations and the unique homes of such networks. on this paper, we provide the primary such works.

1.1 Contributions

In this work, we pose the following research question: if there may be an application wherein messages that need to be exchanged are quick and each their privateness and integrity want to be preserved, can one do better than simply encrypting the messages the use of an encryption set of rules and authenticating them using trendy MAC algorithm? We solution the query with the aid of featuring new strategies for authenticating brief encrypted messages that are greater efficient than existing strategies. in the first technique, we make use of the truth that the message to be authenticated is likewise encrypted, with any comfy encryption algorithm, to append a brief random string to be used inside the authentication method. Since the random strings used for specific operations are impartial, the authentication algorithm can enjoy the simplicity of unconditional secure authentication to permit for quicker and greater green authentication, without the problem to manage one-time keys. within the 2d approach, we make the greater assumption that the used encryption algorithm is block cipher based to in addition enhance the computational efficiency of the first technique. The using purpose in the back of our investigation is that the usage of a preferred motive MAC set of rules to authenticate exchanged messages in such systems may now not be the most efficient answer and might result in waste of resources already available, namely, the safety this is furnished by way of the encryption algorithm.

2 NOTATIONS AND PRELIMINARIES

2.1 Notations

1) We use ZZp as the usual notation for the finite integer ring with the addition and multiplication operations executed modulo p.

2) We use ZZ* p as the standard notation for the multiplicative organization modulo p; i.e., ZZ'^*_p includes the integers that are surprisingly high to p.

3) For two strings a and b of the identical period, (a + b) denotes the bitwise one of a kind-or (XOR) operation.

4) For any two strings a, b, (a3 AUTHENTICATING brief ENCRYPTED MESSAGES in this section, we describe our first authentication scheme that can be used with any IND-CPA secure encryption algorithm. And crucial assumption we make is that messages to be authenticated are no longer than a predefined period. This includes programs in which messages are of constant duration that is regarded a priori, consisting of RFID structures in which tags need to authenticate their identifiers, sensor nodes reporting occasions that belong to certain area or measurements within a positive range and so on. The newness of the proposed scheme is to make use of the encryption algorithm to supply a random string and use it to attain the simplicity and performance of one-time pad authentication

without the need to manipulate impractically lengthy keys.

3.1 The Proposed Machine

Permit N 1 be an upper sure on the duration, in bits, of exchanged messages. This is, messages to be authenticated can be no longer than (N_1)-bit lengthy. Choose p to be an N-bit lengthy top integer. (If N is just too small to offer the favored security stage, p may be chosen big enough to fulfill the required safety degree.) Choose a integer k_s uniformly at random from the multiplicative institution ZZ_p^*; k_s is the name of the game key of the scheme. The high integer, p, and the secret key, ks, are distributed to valid customers and can be used for message authentication. Word that the cost of p need now not be secret, most effective ks is secret. Permit E be any IND-CPA secure encryption algorithm. Let m be quick messages (N 1 bit or shorter) this is to be transmitted to the supposed receiver in a personal manner (by way of encrypting it with E). In preference to authenticating the message using a conventional MAC set of rules, take into account the following technique. On input a message m, a random n_{once} r 2 ZZp is chosen. (We overload m to denote each the binary string representing the message, and the integer representation of the message as an element of ZZp. The equal applies to ks and r. The distinction between the two representations might be overlooked when it's far clean from the context.) We assume that integers representing distinct messages are also wonderful, which may be done via accurately encoding messages.

3.2 Overall Performance Dialogue

There are three classes of well-known message authentication codes that can be used to preserve message integrity in cell and pervasive computing. you may use a MAC based on block ciphers, a MAC based on cryptographic hash features, or a MAC primarily based on prevalent hash-characteristic families. Considering MACs based on standard hashing are acknowledged to be greater computationally efficient than MACs based on block ciphers and cryptographic hash function, we awareness on comparing the proposed MAC to frequent hash functions-based MACs. In MACs based on ordinary hashing, two sections of computations are required: 1) a message compression section using a normal hash feature, and 2) a cryptographic segment in which the compressed picture is processed with a cryptographic primitive (a block cipher or a cryptographic hash feature). The compression section is just like the computation of (4) of the proposed MAC (in fact, the proposed MAC of (4) is an example of strongly regularly occurring hash features). As hostile to conventional accepted hash functions-based MACs, however, there may be no need to process the end result of (four) with a cryptographic function in the proposed method. while the messages to be authenticated are short, the modulus prime, p, can also be small. For a small modulus, the modular multiplication of (4) isn't a time eating operation. That is, for quick messages, the cryptographic section is the maximum time ingesting section. Considering we goal packages wherein messages are brief, casting off the want to carry out one of these cryptographic operation can have a big effect on the overall performance of the MAC operation. For instance, at the same time as 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 of (four) runs in about 1.5 cycles/byte, which illustrates the importance of disposing of the cryptographic section from our MAC. Every other big gain of the proposed approach, especially for low-electricity gadgets, is hardware efficiency. The hardware required to

perform modular multiplication is less than the hardware required to perform state-of-the-art cryptographic operations. As a end result, power consumption is in flip reduced. for instance, at the same time as cryptographic hash functions devour 20-30J/bit, modular multiplication can eat as little as 0:02J/bit. It remains to compare the proposed scheme with single pass authenticated encryption primitives. however, due to the fact that all cozy authenticated encryption primitives are block cipher based totally,2 while the scheme proposed right here can be used along movement ciphers, we put off the evaluation until segment 5, in which we describe a extra green authentication scheme assuming the encryption is block cipher primarily based.

3.3 Safety Version

A message authentication scheme consists of a signing set of rules S and a verifying algorithm V. The signing set of rules is probably probabilistic, while the verifying one is commonly no longer. Associated with the scheme are parameters and N describing the duration of the shared key and the resulting authentication tag, respectively. On enter an ‘-bit key ok and a message m, set of rules S outputs an N-bit string referred to as the authentication tag, or the MAC of m. On enter an ‘-bit key k, a message m, and an N-bit tag, set of rules V outputs a chunk, with 1 standing for receive and 0 for reject. We ask for a basic validity circumstance, namely that real tags are well-known with chance one

In general, an adversary against a message authentication scheme is a probabilistic algorithm A, which is given oracle get admission to to the signing and verifying algorithms S(k,) and V(okay,) for a random however hidden desire of okay. A can question S to generate a tag for a plaintext of its choice and ask the verifier V to verify that is a valid tag for the plaintext. Officially, A’s attack on the scheme is defined via the following test: A random string of the durations‘are chosen because the shared mystery.

The verify queries are allowed because, unlike the putting in digital signatures, A can not compute the verify predicate on its very own (for the reason that affirm set of rules is not public). Notice that a does now not see the secret key k, nor the coin tosses of S. The final results of jogging the experiment inside the presence of an adversary are used to define protection.

3.4 Safety Analysis:

In this section, we show the confidentiality of the machine, give a proper safety evaluation of the proposed message authentication mechanism, and then discuss the security of the composed authenticated encryption system.

3.4.1 Statistical Privateness: We show in this section that the privateness of the proposed compositions is provably secure assuming the underlying encryption set of rules gives in-distinguish-ability under selected plaintext attacks (IND-CPA). Remember an adversary, B, who is given oracle get right of entry to to the encryption algorithm, E. The adversary calls the encryption oracle on a polynomial range of messages of her preference and records the corresponding ciphertexts. The adversary then chooses identical-duration messages, m0 and m1, and gives them to the encryption oracle. The oracle draws a piece $b^2\{0,1\}$ uniformly at random, encrypts m_b, and gives the adversary the ensuing ciphertext.

3.4.2 Data Authenticity

We will now continue with the main theorem formalizing the adversary’s gain of successful forgery against the proposed scheme. Observe also that, except in addition assumptions approximately the encryption algorithm is

assumed (along with the pseudorandom permutation assets as in section 5), it's far vital for the security of authentication to perform the multiplication modulo a top integer. That is, it was proven that the safety of authentication based on common hash families similar to the one in (4) is depending on the used modulus. Mainly, it became proven that the probability of successful forgery is proportional to the reciprocal of the smallest prime component of the used modulus. It is also crucial to observe that, despite the fact that we do assume that message confidentiality is preserved, using an encryption set of rules, knowing the message does now not causes breaking the integrity of the proposed algorithms. As can be seen inside the proof of Theorem 2, message integrity is confirmed to be at ease despite the fact that the adversary is given the ability to launch chosen message attacks.

3.4.3 Safety of the Authenticated Encryption Composition

Bellare and Namprempre defined the notions of integrity for authenticated encryption structures: the primary is integrity of plaintext (INT-PTXT) and the second one is integrity of ciphertext (INT-CTXT). Mixed with encryption algorithms that offer in-distinguish-ability under chosen plaintext assaults (IND-CPA), the security of various techniques for constructing time-honored compositions is analyzed. Be aware that our construction is an instance of the encrypt and authenticate (E&A) standard composition because the plaintext message is going to the encryption algorithm as an enter, and the equal plaintext message goes to the authentication algorithm as an enter. Fig. 1 illustrates the variations between the 3 methods for generically composing an authenticated encryption machine. It was shown that E&A compositions do now not generally provide IND-CPA. that is especially because there exist comfy MAC algorithms that leak statistics approximately the authenticated message (a detailed instance of this type of MAC can be observed). Glaringly, if this sort of MAC is used to compose an E&A gadget, then the authenticated encryption does now not provide IND-CPA. By using Theorem 1, but, the proposed authenticated encryption scheme is as a minimum as private as the underlying encryption algorithm. Because the encryption algorithm is IND-CPA cozy, the ensuing composition presents IND-CPA. Every other end result of [59] is that E&A compositions do no longer offer INT-CTXT. However, the authors additionally factor out that the belief of INT-PTXT is the greater herbal requirement, at the same time as the primary cause of introducing the more potent perception of INT-CTXT is for the security members of the family derived. The purpose why E&A compositions do no longer usually provide INT-CTXT is because there exists secure encryption algorithms with the assets that the ciphertext may be modified without changing its decryption. Glaringly, if such an encryption algorithm is combined with our MAC to compose an E&A composition, best INT-PTXT is carried out (since the tag in our scheme is a feature of plaintext). A sufficient situation, but, for the proposed composition to offer INT-CTXT is to apply a one-to-one encryption algorithm (most sensible encryption algorithm are diversifications, i.e., one-to-one). to see this, have a look at that, with the aid of the one-to-one belongings, any change of the cipher-text will correspond to converting its corresponding plaintext and, through Theorem 2, a changed plaintext will pass undetected with a negligible chance.

4. FROM SUSCEPTIBLE TO ROBUST UNFORGEABILITY

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

As consistent, there are notions of un-forge-ability in authentication codes. Namely, a MAC algorithm can be weakly un-forge-able under chosen message assaults (WUFCMA), or strongly un-forge-able below chosen message assaults (SUF-CMA). A MAC algorithm is stated to be SUFCMA if, after launching chosen message attacks, it is infeasible to forge a message-tag pair in an effort to be ordinary as legitimate regardless of whether or not the message is "new" or now not, as long as the tag has no longer been formerly attached to the message by means of an authorized person. If it's miles simplest hard to forge legitimate tags for "new" messages, the MAC set of rules is stated to be WUF-CMA.

5 ENCRYPTING WITH PSEUDORANDOMNESS

Variations (BLOCK CIPHERS) in this section, we describe a message authentication approach that is quicker than the one defined in preceding sections. the principle concept of this approach is that the input/ output relation of the used encryption operation can be realized as a pseudorandom permutation. In what follows, we are able to show how to make use of the pseudo randomness of block ciphers in a singular way to further enhance the performance of the authentication set of rules of section 3.

5.1 The Proposed gadget

Allow $F:\{0,1\}^N \times \{0,1\}^N$ be the characteristic representing the bock cipher. We assume that F acts as a strong pseudorandom permutation, a standard assumption contemporary block ciphers are believed to fulfill. Anticipate further that exchanged messages are N-bit lengthy.

5.1.1 Message Encryption Permit m to be a quick message this is to be transmitted to the supposed receiver in a private manner. For each message to be transmitted, a random nonce r^2 ZZ_2^N is chosen. (We overload m to denote both the binary string representing the message, and the integer representation of the message as an element of ZZ_2^N ; the equal applies to r. The distinction between the two representations will be ignored while it's far clear from the context.) Now, the concatenation of r and m is going to the encryption algorithm, call it E, as an input. preferably, we can also preference E to be a robust pseudorandom permutation; however, considering the fact that N can be sufficiently long (e.g., 128 or large), building a block cipher that maps 2N-bit strings to 2N-bit strings can be steeply-priced. therefore, we motel to the nicely-studied cipher block chaining (CBC) mode of operation to assemble E from F, as illustrated in Fig. 2.3 Recall the CBC mode of operation depicted in Fig. 2.

The nonce r is treated because the first plain text blocks and is XORed with the initialization vector (IV) to insure INDCPA protection. The primary ciphertext block,

$c_1 = F_{kE}(IV + r)$ (13) is then XORed with the second plaintext block, m in our production, to produce the second one ciphertext block,

$c_2 = F_{kE}(c1 + m)$ (14) where kE is the important thing similar to the block cipher. The ensuing

$$c = E(r, m) = IV\ k_{c1}k_{c2} \qquad (15)$$

is then transmitted to the supposed receiver as the ciphertext.

5.1.2 Message Authentication

With the encryption described above, authentication will become simpler than those in preceding sections; the authentication tag of message m is calculated as follows: Upon

receiving the ciphertext, the supposed receiver decrypts it to extract r and m. Given, the receiver can check the validity of the message by performing the following integrity test: If the integrity test of (17) is glad, the message is considered true. In any other case, the integrity of the message is denied.

5.2 Overall Performance Dialogue

First, we examine the scheme of this section to the scheme of section 3, after which evaluate it to single-pass schemes. Assuming gadgets are already geared up with a cozy block cipher to encrypt messages, the authentication technique of this section requires best one modular addition. At the same time as addition is executed in the O (n) time, the fastest integer multiplication algorithms normally require O(n log n log log n) time. Consequently, as green because the scheme proposed in segment three, the authentication method of this section is at the least O (log n log log n) faster. Complexity analysis, however, can be faulty with the aid of soaking up massive constants. That is certainly the case in comparing the basic scheme of segment 3 to the scheme of this section. For n = 32, the easy addition of this scheme runs in about 0.02 cycles/byte5 in preference to the 1.5 cycles/ byte of the previous scheme. The purpose that the improvement is better than O (log n log log n) is mainly due to the modular reduction. This is, at the same time as discount modulo prime integer is a nontrivial operation, discount modulo 2n may be executed by way of actually stopping at the nth bit.

5.3 Protection Version

Recollect that, to version the security of a message authentication scheme in the fashionable setup, a probabilistic polynomial time adversary, A, is given oracle get admission to to the signing and verifying algorithms, and challenged to generate a brand new rub down-tag pair with a view to be common as legitimate, for a tag that has now not been attached to the message via the signing oracle. Look at, but, that the message to be authenticated in our setup ought to also be encrypted. that is, what the supposed user receives is a ciphertext-tag pair, as opposed to plaintext-tag pair within the trendy version. This means that the adversary must give you a legitimate ciphertext-tag pair for a a hit forgery. In what follows, we modify the usual model of section 2 to cope with the difference between preferred MACs and our MAC in which the message have to be encrypted. Let E be the underlying encryption algorithm. (We treat E as a black box that takes a plaintext message as an enter and outputs its corresponding ciphertext.) The signing oracle internally calls the encryption algorithm and outputs a ciphertext-tag pair. this is, given an encryption set of rules E, on input a key okay and a message m, the signing set of rules

5.4 Safety Analysis

In this section, we prove the privacy of the gadget, provide a formal security evaluation of the proposed message authentication mechanism, and then discuss the safety of the composed authenticated encryption system.

5.4.1 Statistical Privateness

Recall that two portions of facts are transmitted to the intended receiver (the ciphertext and the authentication tag), each of that are functions of the personal plaintext message. Now, in terms of the authentication tag, take a look at that the nonce r serves as a one-time key (just like the position r plays in the construction of segment three). The formal evaluation that the authentication tag does not compromise message

privateness is the same as the one furnished in segment 3.4.1 and, for this reason, is omitted.

5.4.2 Statistical Authenticity

Earlier than we provide a bound on the possibility of successful forgery, we provide a casual discussion on how the shape of the authenticated encryption composition will be utilized. Recall that, in fashionable MACs, the safety is modeled through the adversary's chance of predicting a valid authentication tag for a certain message. that is, given the adversary's understanding of a polynomial wide variety of legitimate message-tag pairs, the purpose of the adversary is to forge a new message-tag pair with a view to be time-honored as legitimate. MACs in an our authenticated encryption composition, then again, are fundamentally specific than fashionable MACs. The intended receiver in an authenticated encryption machine receives a ciphertext-tag pair as adversarial to message-tag pair. this means that, for an tried forgery to achieve success, the adversary should come up with a ciphertext-tag pair in an effort to be normal as valid, not a message-tag pair.

6. END

On these works, a brand new method for authenticating quick encrypted messages is proposed. The fact that the message to be authenticated need to also be encrypted is used to deliver a random nonce to the intended receiver through the ciphertext. This allowed the design of an authentication code those blessings from the simplicity of unconditionally cozy authentication without the want to manipulate one-time keys. In particular, it's been demonstrated on this paper that authentication tags may be computed with one addition and a one modular multiplication. For the reason that messages are relatively quick, addition and modular multiplication can be executed quicker than present computationally at ease MACs inside the literature of cryptography. whilst gadgets are equipped with block ciphers to encrypt messages, a 2d technique that utilizes the reality that block ciphers can be modeled as sturdy pseudorandom variations is proposed to authenticate messages the use of a unmarried modular addition. The proposed schemes are shown to be orders of significance faster, and eat orders of importance less energy than traditional MAC algorithms. consequently, they are extra suitable to be used in computationally limited cell and pervasive devices.

REFERENCES

[1] L. Carter and M. Wegman, "Universal Hash Functions," J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.

[2] 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.

[3] V. Shoup, "On Fast and Provably Secure Message Authentication Based on Universal Hashing," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 313-328, 1996.

[4] 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.

[5] B. Alomair and R. Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels," IEEE Trans. Computers, 2012.

[6] Federal Information Processing Standards (FIPS) Publication 113, Computer Data Authentication, FIPS, 1985.

[7] ISO/IEC 9797-1:1999 Standard, Information Technology – Security Techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms Using a Block Cipher, ISO/IEC, 1999.

[8] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," 2005.

[9] T. Iwata and K. Kurosawa, "OMAC: One-Key CBC MAC," Proc. Int'l Conf. Fast Software Encryption (FSE '03), pp. 129-153, 2003.

Mr. Amirishetty Raju earned M.Tech CSE from JNTU Hyderabad, Presently, working at Vaagdevi College of Engineering as Assistant Professor. His active research interests include networks, adhoc networks and distributed systems.

Mail id: testraju76@gmail.com

Mrs. Vadlakonda Niharika is pursuing M.Tech degree in Computer Science and Engineering in CSE Department in Vaagdevi College of Engineering and Telangana state, India .

Mail id: niha.goud@gmail.com