Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.467 – 475

RESEARCH ARTICLE

AN ELLIPTIC CURVE CRYPTOGRAPHY BASED ENHANCED ADAPTIVE ACKNOWLEDGMENT (ECC-EAACK) INTRUSION DETECTION SYSTEM

[1]Deboral C, [2]Sudhagar G

[1]PG Scholar, Department of Computer Science and Engineering, Anna University Chennai, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India

[1,2]Ranganathan Engineering College, Coimbatore

[1] deboral.cse33@gmail.com, [2] sudhakar.g7018@gmail.com

Abstract **-** ***MANET is a new wireless network technology increasingly used in many applications. These networks are more vulnerable to attacks than wired networks. Since they have different characteristics, conventional security techniques are not directly applicable to them. Intrusion detection system (IDS) is one of the most active fields of research in Mobile Ad-hoc Network's (MANET) field. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. Packet-dropping attack has always been a major threat to the security in MANETs. In this research work, novel IDS named EAACK protocol using ECC is specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. In this paper, we propose and implement a new intrusion-detection system named Elliptic Curve Cryptography Based Enhanced Adaptive ACKnowledgment (ECC-EAACK) specially designed for MANETs demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.***

Keywords – Digital signature, Elliptic curve cryptography algorithm (ECC), Mobile Ad hoc NETwork (MANET), Enhanced Adaptive ACKnowledgment (EAACK)

I. INTRODUCTION

Wireless networking is now the medium of choice for many applications. In addition, modern manufacturing techniques allow increasingly sophisticated functionality to reside in devices that are ever smaller, and so increasingly mobile. Mobile ad hoc networks (MANETs) combine wireless communication with a high degree of node mobility. Limited range wireless communication and high node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met[1],[2]. The dynamic nature of the protocols that enable MANET operation means they are readily suited to deployment in extreme or volatile circumstances. MANETs have consequently become a very popular research topic and have been proposed for use in many areas such as rescue operations, tactical operations, environmental monitoring, conferences, and the like [3]. MANETs by their very nature are more vulnerable to attack than wired networks. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices introduces new security risks [4],[5]. As part of rational risk management we must be able to identify these risks and take appropriate action. In some cases we may be able to design out particular risks cost-effectively. In other cases we may have to accept that vulnerabilities exist and seek to take appropriate action when we believe someone is attacking us [6]. As a result, intrusion detection is an indispensable part of security for MANETs.

Many intrusion detection systems (IDS) have been proposed in the literature for wired networks but MANETs specific features make direct application of these approaches to MANETs impossible[7],[8]. New approaches need to be developed or else existing approaches need to be adapted for MANETs. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure; it is not adequate or cost effective [9]. The absence of a central coordinator and base stations makes operations in MANETs more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks [10]. Security issues of MANETs in group communications are even more challenging because of the involvement of multiple senders and multiple receivers.

II. RELATED WORK

A. *IDS* in *MANET*s

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of IDS are data collection, detection, and response. The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module. IDS can use different data sources as inputs to the system: system logs, network packets, etc. In the detection component data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component. In the literature, three intrusion detection techniques are used.

1) Anomaly-Based

The first technique is anomaly-based intrusion detection which profiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviours. Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data mining and neural networks. Defining normal behaviour is a major challenge. Normal behavior can change over time and intrusion detection systems must

be kept up to date. False positives the normal activities which are detected as anomalies by IDS can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly.

2) Misuse-Based

Misuse-based intrusion detection compares known attack signatures with cur-rent system activities. It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate. The drawback of this approach is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. Therefore, both techniques are generally employed for effective intrusion detection.

3) Specification-Based

The last technique is specification-based intrusion detection. In this approach, a set of constraints on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with a lower false positive rate. It can detect new attacks that do not follow the system specifications. Moreover, it does not trigger false alarms when the program or protocol has unusual but legitimate behavior, since it uses the legitimate specifications of the program or protocol. It has been applied to ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol) and many MANET routing protocols. Defining detailed specifications for each program/protocol can be a very time consuming job. New specifications are also needed for each new program/protocol and the approach cannot detect some kind of attacks such as DoS (Denial of Service) attacks since these do not violate program specifications directly.
When an intrusion is detected, an appropriate response is triggered according to the response policy. Responses to detected *intrusions* can be passive or active. Passive responses simply raise alarms and notify the proper authority. Active responses try to mitigate effects of intrusions and are divided into two groups: those that seek control over the attacked system, and those that seek control over the attacking system. The former tries to restore the damaged system by killing processes, terminating network connections, and the like. The latter tries to pre-vent attacker's future attempts, which can be necessary for military applications.

III. PROPOSED SYSTEM

We propose a strong and light-weight Intrusion detection mechanism called EAACK which requires less hardware cost. EAACK is consists of three major parts called: ACK, S-ACK and MRA.
ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. According to this method, if the receiver node does not send the ACK within predefined period, then ACK assumes malicious may present and switch to S-ACK part to detect them.
In S-ACK part, for every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power. If malicious found, then MRA part suggests alternate path to the destination. Unlike the TWOACK scheme, where the source node immediately trusts the misbehavior report, EAACK requires the source node to switch to MRA node and confirm this misbehavior report. This is a vital step to detect false misbehavior report in our proposed scheme.

To initiate the MRA mode, the source node first searches its local knowledge base and seeks for an alternative route to the destination node. If there is no other that exists, the source node starts a routing request to find another route. Due to the nature of MANETs, it is common to find out multiple routes between two nodes. When the destination node receives an MRA packet, it searches its local knowledge base and compares if the reported packet was received, then it is safe to conclude that this is a false misbehavior report and whoever generated this report is marked as malicious.

Instead of RSA, Improved Cryptographic technique or Improved ECC is going to use. Improves intrusion detection result in MANET. It ensures the secure communication of data packets in the network. Increased security and convenience. Provides digital signatures that cannot be repudiated. High speed while performing in software. Digital signature is a widely adopted approach to ensure the authentication, integrity, and non-repudiation of MANETs. It can be generalized as a data string, which associates a message (in digital form) with some originating entity, or an electronic analog of a written signature.

IV. SCHEME DESCRIPTION

The approach described in this research paper is based on our previous work, where the backbone of EAACK was proposed and evaluated through implementation. In this paper, we extend it with the introduction of digital signature to prevent the attacker from forging acknowledgment packets. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In our proposed scheme, we assume that the link between each node in the network is bidirectional. Furthermore, for each communication process, both the source node and the destination node are not malicious. Unless specified, all acknowledgment packets described in this research are required to be digitally signed by its sender and verified by its receiver.

EAACK is an acknowledgment-based IDS. All three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable. With regard to this urgent concern, we incorporated digital signature in our proposed scheme. In order to ensure the integrity of the IDS, EAACK requires all acknowledgment packets to be digitally signed before they are sent out and verified until they are accepted. However, we fully understand the extra resources that are required with the introduction of digital signature in MANETs. To address this concern, we implemented both DSA and RSA digital signature schemes in our proposed approach. The goal is to find the most optimal solution for using digital signature in MANETs.

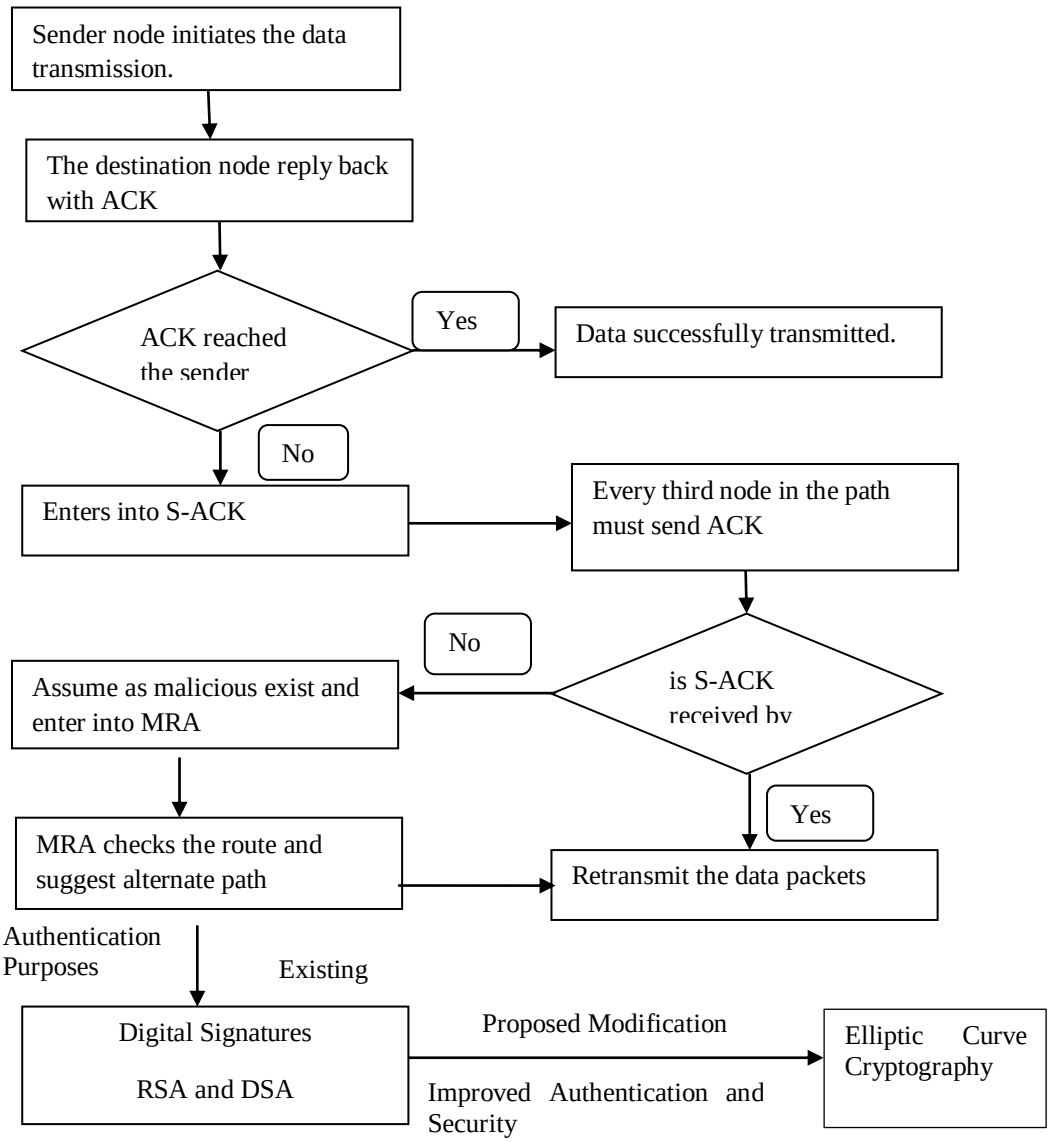

Fig. 1 System architecture

V. PERFORMANCE EVALUATION

Our simulation environment and methodology as well as comparing performances through simulation result comparison with Watchdog, TWOACK, EAACK schemes (without ECC) and EAACK with ECC. In order to measure and compare the performances of our proposed scheme, we continue to adopt the following two performance metrics [13].

Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

A. Simulation Results-Scenario 1 [Delay]

The average time it takes a data packet to reach the destination which includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. Metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as: Avg. D=S/N Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the all destination nodes.

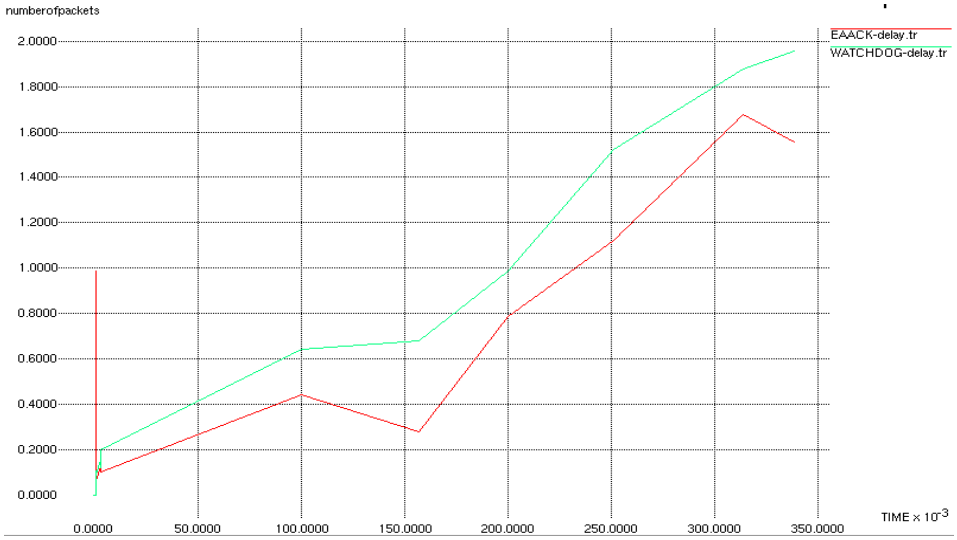

Fig. 2 Comparison of delay

B. Simulation Results-Scenario 2 [Throughput]

Throughput is defined as the total number of packets delivered over the total simulation time. Mathematically, it can be defined as: Throughput= N/1000 Where N is the number of bits received successfully by all destinations. Performance of the watchdog is decreasing while the throughput of EACCK is increasingly regularly.

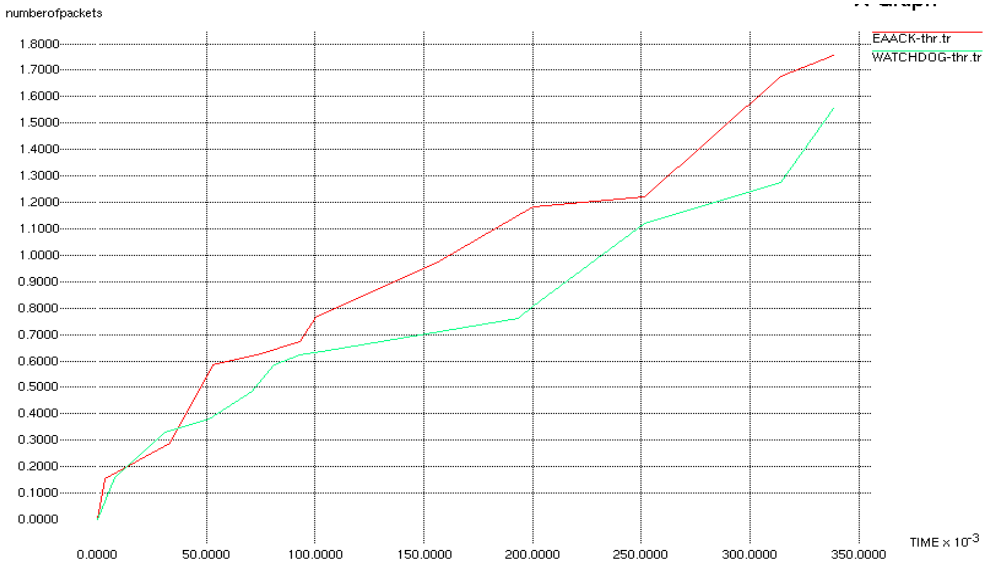

Fig. 3 Comparison of throughput

C. Simulation Results-Scenario 3 [Packet Delivery Ratio]

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as: PDR= S1 / S2 , Where S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes. Performance of the Watchdog is reducing regularly while the PDR is increasing in the case of EACCK. EACCK is better among the other IDS schemes.

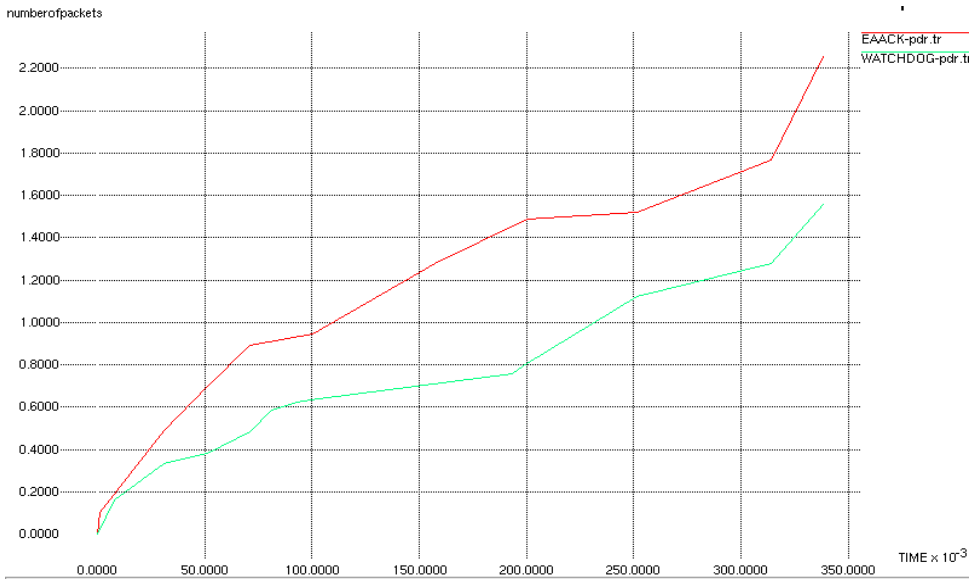

Fig. 4 Comparison of Packet Delivery Ratio

VI. CONCLUSION

Intrusion detection system (IDS) is one of the most active fields of research in Mobile Ad-hoc Network's (MANET) field. This systems are usually focused on detecting problems with the routing systems to prevent DoS and Man-in-the-middle and, despite of the amount of papers written which try to solve, many of them are just theoretical and have only been proved in simulations. Packet dropping attack has always been a major threat to the security in MANETs. A novel IDS named EAACK protocol specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehavior report. In order to seek the optimal DSAs in MANETs, we implemented ECC schemes in our simulation. Eventually, we arrived to the conclusion that the ECC scheme is more suitable to be implemented in MANETs than DSA and RSA.

REFERENCES

[1]. K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technology," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[2]. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3]. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.

[4]. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer- Verlag, 2008.

[5]. L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6]. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.

[7]. V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[8]. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Comput. Syst. Appl., 2002, pp. 3–13

[9]. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.

[10]. G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Comput. Sci., vol. 3, no. 8, pp. 574–582, 2007.

[11]. K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323,2004.

Authors Profile

Deboral C – Currently pursuing her M.E in Computer Science and Engineering from Ranganathan Engineering College, Coimbatore. Her areas of interest are network security, and Mobile computing.

G. Sudhakar – He is working as an Assistant Professor in Dept.of Computer Science and Engineering in Ranganathan Engineering College, Coimbatore, India. His areas of interest are network security, Mobile computing, and Cloud computing.

