ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ

ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ

КАТЕДРА „КОМУНИКАЦИОННИ МРЕЖИ“

маг. инж. Шайк Джейвид Рашийд

Сигурни и ефективни методи базирани на криптографията с елиптични криви за защита на транзакциите за електронна търговия

АВТОРЕФЕРАТ

на дисертация за присъждане на образователна и научна степен

„ДОКТОР“

Област на висше образование: 5. Технически науки

Професионално направление: 5.3 Комуникационна и компютърна техника

Научна специалност: Комуникационни мрежи и системи

Научен ръководител: проф. д-р инж. Георги Любенов Илиев

София, 2019

Дисертационният труд е обсъден и насочен за защита от Катедрения съвет на катедра „Комуникационни Мрежи“ към Факултет по Телекомуникации при Технически Университет – София на редовно заседание, проведено на 03.12.2018 г.

Публичната защита на дисертационния труд ще се състои на 25.03.2019 г. (понеделник) от 13,00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със заповед № ОЖ-53-18 от 19.12.2018 г. на Ректора на ТУ-София в състав:

1. Проф. д-р инж. Владимир Костадинов Пулков – председател
2. Проф. д-р инж. Георги Любенов Илиев – научен секретар
3. Проф. д-р инж. Борис Петков Цанков
4. Проф. д-р инж. Георги Костов Стоянов
5. Доц. д-р инж. Олимпия Николаева Роева

Рецензенти:

1. Проф. д-р Владимир Костадинов Пулков
2. Доц. д-р Олимпия Николаева Роева

Материалите по защитата са на разположение на интересуващите се в кабинет 1254, блок 1, Технически Университет – София.

Дисертантът е задочен докторант към катедра „Комуникационни Мрежи“, Факултет по Телекомуникации. Изследванията по дисертационният труд са направени от автора, като резултатите от тях са публикувани.

Автор: маг. инж. Шайк Джейвид Рашийд

Заглавие: Сигурни и ефективни методи базирани на криптографията с елиптични криви за защита на транзакциите за електронна търговия

Тираж: 30 броя

Отпечатано в ИПК на Технически университет – София

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Електронната търговия може да бъде широко определена като модел на продажба и покупка, при който купувачите могат да участват във всички фази на решение за покупка, като същевременно преминават през тези процеси по електронен път, а не във физически магазин. Тъй като мащабът на електронните търговски транзакции нарасна, той стана много привлекателен за престъпниците, а обемът на измамни електронни търговски транзакции бързо нараства. Поради това се наблюдава увеличаване на вниманието, отделено на сигурността на платежните системи, използвани за обработка на онлайн транзакции. За да заработи системата за електронна търговия, сигурността и поверителността в Интернет са два основни проблема [1]. Много потребители, които правят онлайн бизнес, се притесняват за личната си информация при онлайн плащанията поради липса на доверие по отношение на въпросите за сигурността в рамките на електронната търговия [3]. Заедно с въпросите, свързани със сигурността и поверителността, електронната търговия също е изправена пред проблемите, свързани с различните видове онлайн атаки. Една широко разпространена и важна атака, която оказва по-значително влияние върху бизнеса за електронна търговия до момента, е атаката отказ от услуга (DoS). Атаката DoS обикновено причинява значителна загуба на приходи от бизнеса за електронна търговия. Въпреки че са разработени различни техники за борба с атаките DoS, по-голямата част от съществуващите техники не се използват поради лошото им качество на работа. Настоящият труд предлага нови техники за автентикация и оторизация, с които е възможно да се облекчат DoS атаките по време на електронната търговия.

Цел на дисертацията, основни задачи и методи на изследване

Основната цел на дисертационния труд е: Да се разработи и развие сигурен, ефикасен, прост и надежден механизъм за автентикация, който би могъл да се използва в приложенията за електронна търговия с ограничени ресурси, които имат високи изисквания за сигурност и да се проектира сигурна и надеждна техника за оторизация за защита на транзакциите при електронна търговия от атаки DoS. За да се постигне тази цел, трябва да се изпълнят следните задачи:

1. Да се проучат различните изисквания за сигурност на системите за електронна търговия заедно с наличните решения за сигурност и да намерят критичните области в електронната търговия, където е необходимо подобрение на сигурността.

2. Да се подобри цялостната сигурност на електронната търговия, като се предложи модел на система за електронна търговия, като се използват усъвършенствани криптографски алгоритми, които имат по-малка изчислителна сложност и осигуряват по-високо ниво на сигурност. Тази задача може да бъде

постигната чрез намиране на подходящи елиптични криви за прилагане на различни ECC алгоритми като ECDH и ECDSA.

3. Да се разработи бърз, сигурен и ефективен механизъм за автентикация на потребителя в системата за електронна търговия, при която потребителят желае да осъществява отдалечен достъп до сървъра чрез своята смарт карта. Предложената техника за автентикация да се използва в приложения, където изискването за сигурност е високо и то да може да бъде защитено срещу различни атаки като ответна атака, атака срещу представяне под чужда самоличност, атака "човек в средата" и т.н.

4. Чрез въвеждане на нов класификатор да се създаде и развие солиден механизъм за откриване на атака отказ от услуга по време на сделките за електронна търговия. Предложената техника трябва точно и прецизно да класифицира оторизирания потребител и неоторизирания потребител по време на сделка за електронна търговия.

Методологията на изследване в дисертацията включва използването на цифрови и симулационни подходи. Предложеният нов модел за сигурност използва ECC като криптографски алгоритъм, който е полезен за гарантиране на сигурността на плащането от страна на клиентите, както и на информацията за поръчки при извършване на бизнес за електронна търговия. Анализът на ефективността на стандартните елиптични криви е полезен, за да се определи подходящата крива за използването на ECC в приложенията за електронна търговия с ограничени ресурси. Предложеният протокол за автентикация на потребител използва криптографията на елиптичните криви, като той е по-сигурен и ефикасен от наличните протоколи за автентикация на потребителите. Използвайки протокола за удостоверяване на автентичността, потребителят може дистанционно да осъществява надежден достъп до автентичния сървър, като по време на този процес се добавя по-малък изчислителен товар към системата. Разработена е техника за откриване на DoS атаки в транзакциите за електронна търговия с помощта на предложения GSO-SVNN класификатор. Предложеният класификатор е проектиран чрез модифициране на SVNN, като се използва алгоритъм GSO, така че теглата да се избират оптимално. Предложеният GSO-SVNN алгоритъм класифицира потребителя като автентичен потребител или атакуващ въз основа на извлечената информация. За да се оцени ефективността на предложената техника експерименталните изследвания са извършени с помощта на четири показателя: точност, прецизност, чувствителност и FPR. За целите на анализа и експериментите се използва MATLAB.

Научна новост

Научната новост в тази дисертация е свързана с предлагането на нови протоколи и техники за подобряване на сигурността на приложенията за електронна търговия чрез осигуряване на механизми за автентикация и оторизация. Анализът на различни елиптични криви се извършва, за да се установи подходящата крива за реализация на ECC в приложенията за електронна търговия с ограничени ресурси. Трудът също така

предлага усъвършенстван протокол за автентикация на потребител на базата на смарт карта, който може да осигури сигурен достъп до отдалечен сървър. Надеждната и усъвършенствана техника за откриване на DoS атаки е разработена и изследвана в мрежа за електронна търговия. Техниката е разработена за откриване на DoS атаки в транзакциите за електронна търговия, като се използва предложения GSO-SVNN класификатор. Предложеният класификатор е проектиран чрез модифициране на SVNN чрез алгоритъм GSO и дава най-добри резултати в сравнение с други подобни техники.

Практическа приложимост

Всички разработени протоколи, както и предложената техника за откриване на DoS атаки, са изследвани и анализирани чрез използване на симулационни експерименти. Направено е сравнение с други техники, които имат подобни функции и характеристики или имат подобни цели по отношение на подобряването на тяхната работа.

Публикуване на резултатите от изследванията в дисертацията

Анализът, предложените подходи и получените резултати за периода 2016 ÷ 2019 са представени в общо 7 авторски публикации, 5 от които на международни конференции, а другите 2 в международни научни списания. Една от публикациите е самостоятелна, а останалите 6 са със съавтори. Международните конференции са: Global Wireless Summit (GWS) 2016; International Scientific Conference on Information, Communication and Energy System and Technologies (ICEST) 2017; IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2017; IEEE International Conference on Computing for Sustainable Global Development (INDIACom) 2018; Springer International Conference on Manufacturing, Advanced Computing, Renewable Energy and Communication (MARC) 2018. Международните научни списания са: International Journal of Current Advanced Research (IJCAR) 2017; International Journal of Current Engineering and Scientific Research (IJCESR) 2018.

Структура и обем на дисертационния труд

Дисертацията е написана на английски език и има обем от 148 страници формат А4 и съдържа увод, четири глави, заключение с изложени основни приноси, списък с фигури, списък с таблици, списък на използваните съкращения, списък на публикациите на автора, списък на използваната литература. Трудът съдържа 50 фигури, 13 таблици и 34 математически израза. Използвани са 114 литературни източника, всичките на латиница, от които 82% са публикувани през последните десет години. Номерата на фигурите и таблиците в автореферата съответстват на тези в дисертацията.

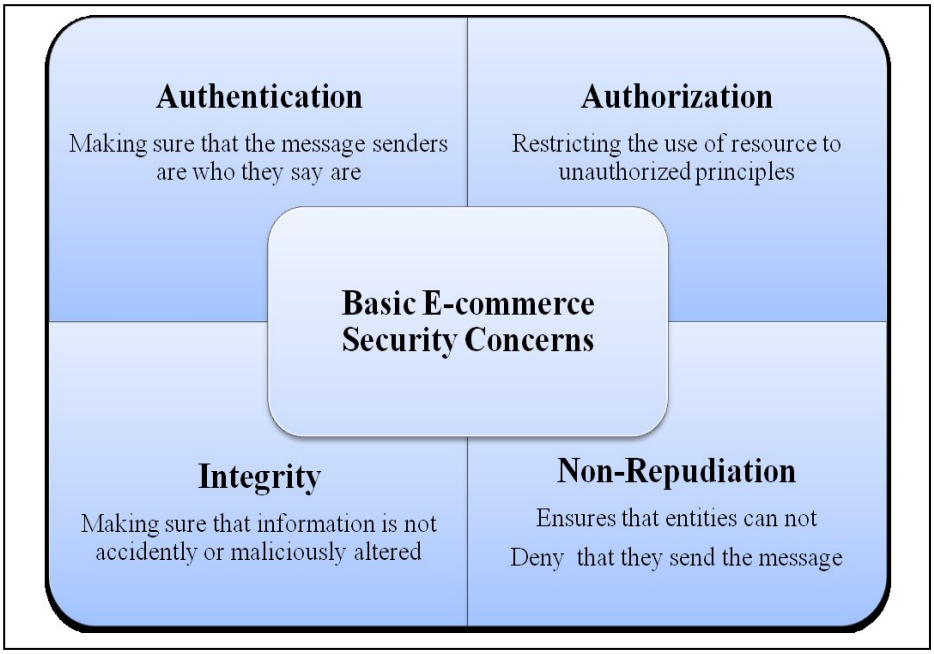
II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1. Състояние на проблема

1.1. Литературно проучване на въпросите за сигурността на електронната търговия и наличните решения

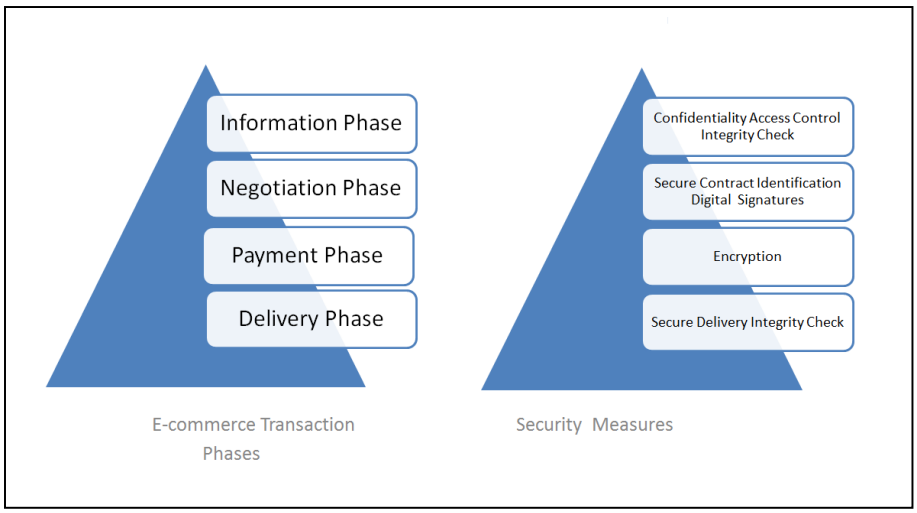
Една от най-популярните дейности в Интернет е онлайн пазаруването. Тя е много гъвкава защото може да пазарувате по ваше желание, по всяко време и навсякъде. Съгласно стандартното определение всички търговски дейности, извършвани чрез Интернет, се наричат общо "електронна търговия" [7]. Първоначално терминът "Електронна търговия" означава процеса на осъществяване на търговските сделки по електронен път с помощта на технологии като Електронен обмен на данни (EDI) и Електронен превод на средства (EFT), с които потребителят може да получи възможност да обменя бизнес информация и извършва електронни транзакции. Поради виртуалността на електронната търговия и тъй като тя е отворена в Интернет, се появяват проблемите със сигурността които са пречка за нейното развитие [11]. Сигурността на електронната търговия като цяло е част от информационната сигурност и се прилага към фактори като компютърна сигурност, сигурност на данните и други фактори за сигурност на информацията. Използването на електронната търговия се увеличава, но не достига потенциала си поради заплахите за конфиденциалността и проблемите със сигурността, които са станали проблеми от голямо значение за както за потребителите, така и за доставчиците на онлайн услуги [1] [26] [27]. Въпросите за сигурността и конфиденциалността е необходимо да се разглеждат в социална, организационна, техническа и икономическа перспектива. Сигурността е също така основна грижа за сайтовете за електронна търговия и техните клиенти. Клиентите, както и сайтовете за електронна търговия, се опасяват от свързаните с това финансови загуби. Защитата на компютърните мрежи, сигурността на търговските транзакции и сигурността на информацията са сериозни проблеми в системите за електронна търговия [30] [31].

През последните няколко години изчислителните облачни технологии са широко приети като алтернативен начин за бизнеса да съхранява данни, да комуникира и да работи. Увеличаването на броя на редица приложения за електронна търговия, използващи изчислителни облачни технологии, предизвиква множество изследвания в областта на сигурността и поставя важни предизвикателства, включително проверка на целостта, удостоверяване на автентичността, контрол на достъпа, предотвратяване на атаки и т.н., които по същество са актуални проблеми за да се направи модерната мрежова среда по-сигурна от преди [34]. Фиг.1.3. показва схематичното представяне на основните опасности за сигурността, свързани с електронната търговия. Ако основните заплахи и изисквания са анализирани внимателно, тогава това помага в изграждането на стабилна архитектура за сигурност на системата за електронна търговия.



Фигура 1.3. Основни параметри за сигурността на електронната търговия

Стратегиите за сигурност на електронната търговия се занимават с два проблема: единият е защита на целостта на бизнес мрежата и нейните вътрешни системи, а вторият е постигането на сигурност на транзакциите между клиента и бизнеса. Сигурността на електронната търговия има свои специфични нюанси и е един от най-видимите компоненти за сигурност, които оказват влияние върху крайния потребител чрез ежедневното взаимодействие с бизнеса. Има много фази на сделка за електронна търговия и всяка фаза има различни мерки за сигурност [47]. Графичната форма на фазите на транзакциите за електронна търговия и мерките за сигурност е изобразена на фиг.1.5.



Фигура 1.5 Мерки за сигурност в различните етапи на електронната търговия [A1]

1.2. Изследване на атака DoS / DDoS и нейното въздействие върху системата за електронна търговия

Атаката DoS е злонамерен опит да се направи сървър или мрежов ресурс недостъпни за потребителите, обикновено чрез временно прекъсване или спиране на услугите на хост, свързан към Интернет [53]. Най-сериозните атаки са "Distributed DoS" (DDoS), при които входящият трафик идва от хиляди уникални IP-и адреси от Botnets или от отразени атаки. DoS атаките могат да навредят на електронната търговия по два начина. Първо, когато търговецът не може да обслужва своите клиенти, търговецът губи рекламни приходи и продажби, а на второ място, клиентите на търговеца, рекламодателите и инвеститорите са разочаровани и поради това могат да търсят конкурентни алтернативи. Според изследването на Corero Network Security 2016 DDoS, загубата на доверие и увереност на клиентите е най-вредното последствие от атака DDoS. Приблизително една трета (32%) от респондентите от изследването са посочили, че DDoS атаки в мрежата им се появяват ежеседмично или дори ежедневно [57].

1.3. Заключение

В областта на електронната търговия сигурността, конфиденциалността и доверието са основните проблеми както за потребителя, така и за търговците. Сигурността на електронната търговия е защитата на активи за електронна търговия от неоторизиран достъп, използване, промяна или унищожаване. Елементите на сигурността на електронната търговия са цялостност, неотхвърляне, автентичност, конфиденциалност и достъпност. Понастоящем защитните стени, технологията за шифроване на данни и технологията за скриване на информация се използват широко в сигурността на електронната търговия. Традиционните техники за криптиране добавят изчислителен товар към системата за електронна търговия. Въпреки многото изминали години от въвеждането на електронната търговия, все пак има съществени проблеми свързани със сигурността. Заедно с въпросите, свързани със сигурността и поверителността, електронната търговия е изправена пред проблемите, дължащи се на различни онлайн атаки. Една широко разпространена атака, която оказва значително влияние върху бизнеса за електронна търговия до момента, е атаката DoS, която води до значителна загуба на приходи. Тази глава подчертава въздействието на атаките DoS и DDoS върху сигурността на електронната търговия и свързаните с нея техники, прилагани в областта на кибернетичната сигурност, заедно с основните предизвикателства.

1.4. Приноси към Глава 1

Тази глава има следните два приноса.

- Представено е подробно проучване относно електронната търговия и нейните проблеми със сигурността, като се вземат предвид изискванията за сигурност на различни нива и наличните инструменти за сигурност. В проучването са разгледани въпросите за сигурността на електронната търговия и наличните решения от началните етапи на тяхното развитие.

Въздействието на атаките DoS и DDoS върху електронната търговия и наличните мерки за противодействие също се анализират.

- В резултат на актуалния анализ са определени основните изисквания за сигурност на електронната търговия и въз основа на това проучване са формулирани целта и задачите на дисертационния труд.

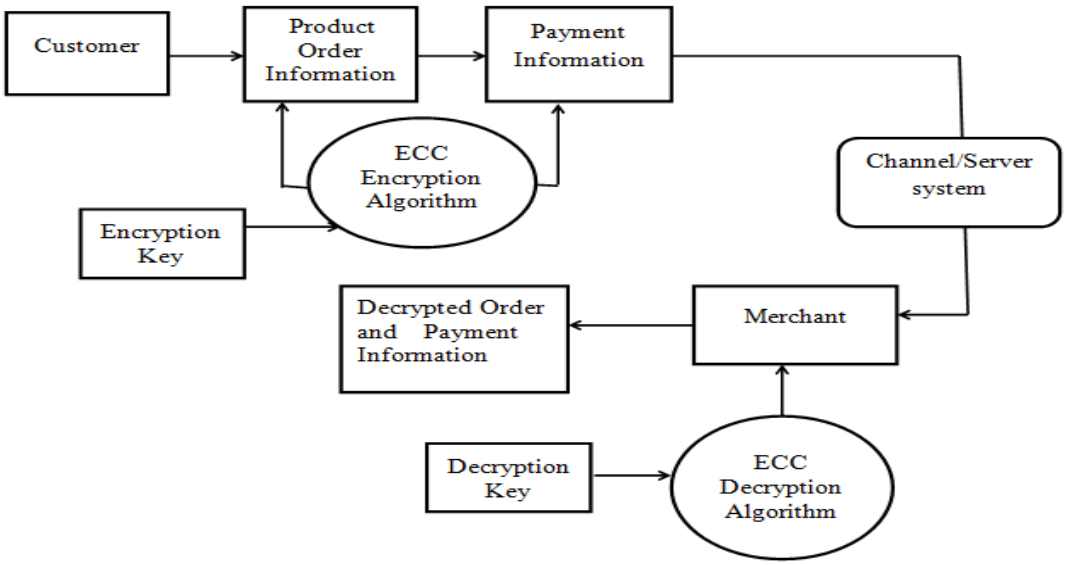
ГЛАВА 2. Подобряване на сигурността на системите за електронна търговия, използвайки криптографията на елиптичните криви

Основното изискване за всяка транзакция за електронна търговия е поверителността на данните, което се постига с помощта на различни техники за криптиране. За да се изпълни изискването за сигурност на електронната търговия се използва широко алгоритъмът за криптография RSA. В случая на RSA размерът на ключа се увеличава пропорционално с изискването за сигурност. RSA е уязвим за много атаки, като Integer Factoring Attacks, Wiener's Attack, Hastad Broadcasting Attack и др. [61]. Поради това ограничение на RSA алгоритъма, нова криптографска схема с публичен ключ, известна като ECC, се очертава като добра алтернатива на RSA. За да се подобри сигурността в бизнеса за електронна търговия, се предлага общ модел за сигурност, като се прилага ECC. В предлагания модел за сигурност заедно с платежната информация може да се осигури конфиденциалност и на информацията за поръчката за покупка на клиента и да се намали изчислителната сложност. При въвеждането на ECC важен фактор е изборът на правилната елиптична крива, защото ако е избрана неподходяща елиптична крива, тогава сигурността на системата е застрашена. За да се разбере кой тип крива е подходящ за използване в ECC в приложенията за електронна търговия, в раздел 2.2 се извършва анализ на различни стандартни елиптични криви. За целите на анализа се разглеждат различни елиптични криви, които се препоръчват от различните криптографски стандарти.

2.1 Проектиране на модел за сигурност за система за електронна търговия, използваща криптографията на елиптичните криви

Защитата на данните при електронната търговия от неразрешен достъп, тяхната промяна или унищожаване е основна задача за осигуряване на сигурността и това се постига чрез различни криптографски техники. Повечето от приложенията за електронна търговия използват RSA алгоритъм за криптиране и декриптиране на тайния ключ. Тъй като криптоанализът става все по-добър, размерът на симетричния и на публичния ключ трябва да се увеличи пропорционално, за да се осигури по-добра сигурност. За алгоритъма RSA NIST препоръчва да се използва ключ с размер от 2048 бита до 2030 г. и увеличаване на размера на ключа до 3072 бита след това за по-добра сигурност [62]. Причината за популярността на ECC техниката е, че с минимална дължина на ключа тя осигурява по-добра сигурност от RSA. ECC изисква 160-битова дължина на ключа в сравнение с 1024-битовата дължина на ключовете на RSA и предлага същото ниво на сигурност [60]. Затова в тази глава ECC, която е криптираща

техника с асиметричен ключ, се анализира като алтернатива на RSA. Ефективността на алгоритъма се измерва с изчислителните ресурси, които консумира. Авторите в [67] реализират ECC и RSA върху хардуер и установяват, че превъзходството в производителността на ECC над RSA се увеличава с намаляването на размера на компютърната дума на процесора. Ако се търси добро хардуерно решение за малки устройства, в сравнение с RSA, ECC има предимството на по-малки размери на ключовете, по-бързо изчисление, както и спестяване на памет, енергия и честотна лента. В тази глава е създаден модел за сигурност на бизнеса в областта на електронната търговия, представен на фиг.2.4. По принцип в електронната търговия фокусът е върху сигурността на платежната информация, но информацията за продукта на клиента не е толкова сигурна. В предлагания модел за защита ECC се използва за осигуряване на сигурността на информацията за поръчка за плащане и покупка на клиента. Една и съща криптосистема с елиптични криви се използва за криптиране на информацията за плащане на клиента и информацията за поръчката. Кодираната информация може да бъде декриптирана само от търговец, който има ключ за декриптиране ECC (частен ключ на ECC).



Фигура 2.4. Предложен модел за сигурност

2.2 Анализ на стандартните елиптични криви за реализация на криптографията на елиптичните криви в приложения за електронна търговия

Най-важният въпрос при използването на ECC е избора на правилната елиптична крива. Съществуват различни видове елиптични криви, предложени от различни стандарти. Изборът на кривата зависи от различните параметри като размер на основното поле, формата на кривата и т.н. В тази част от дисертацията се избират множество елиптични криви, препоръчани от различни стандарти за криптография, които се анализират, фокусирайки се върху ефективността и защитните елементи. Анализът се извършва, като се изследва всяка крива за реализиране на ECDH и ECDSA,

които са общи алгоритми използвани в ECC. Ефективността на всяка крива се измерва по отношение на времето за изчисление, което е необходимо за различните ECC алгоритми. Представена е сравнителна таблица, като се има предвид изчислителното време необходимо на всяка крива за извършване на различни операции.

A. ECDH алгоритъм

ECDH е по-скоро протокол за ключово споразумение, отколкото алгоритъм за криптиране. ECDH дефинира как се генерират и обменят ключовете между двете страни. Всяка избрана крива се използва в основното си поле p, предложено от нейния стандарт. Една произволна точка P е избрана от кривата. За да се обменят ключовете между Алис и Боб, използвайки ECDH, се приема следната процедура.

Стъпка 1: Алис и Боб генерират свои собствени частни и публични ключове.

Стъпка 2: Алис има частен ключ $A(K_{Pr})$ = 'a' и публичен ключ $A(K_{Pb}) = a*P$. Боб има частен ключ $B(K_{Pr})$ = 'b' и публичен ключ $B(K_{Pb}) = b*P$.

Стъпка 3: Публичните ключове $A(K_{Pb})$ и $B(K_{Pb})$ на Алис и Боб се обменят по несигурен канал.

Стъпка 4: „Човекът в средата" може да прихване a*P и b*P, но няма да може да открие нито a, нито b, без да реши проблема с дискретния логаритъм.

Стъпка 5: От двете страни Алис изчислява за възстановяване на споделените ключове S = a*(b*P), и Боб изчислява S = b*(a*P). Споделената тайна S е еднаква както за Алис, така и за Боб.

$$S = a*(b*P) = b*(a*P) = a*b*P$$

B. ECDSA алгоритъм

ECDSA се използва за подписване на хеша на съобщението. Хешът на съобщението се съкращава, за да направи дължината на битовете на хеша същата като дължината на битовете на n, което е редът на подгрупата [78]. Съкратеният хеш е цяло число и се обозначава като z. Простото число q, елиптична крива E mod q, точката G, която е основната точка от кривата, частният ключ "d" на Alice и публичният ключ H_A се използват за реализация на ECDSA между Alice и Bob. Алгоритъмът ECDSA, изпълняван от Алис, за да подпише съобщението, работи както следва.

Стъпка 1: Взема се произволно цяло число k от {1,…,n−1} (където n е редът на подгрупата).

Стъпка 2: Изчислява се точката P=k*G.

Стъпка 3: Изчислява се $r = x_P \bmod n$ (където x_P е координата x на P).

Стъпка 4: Ако r = 0, тогава се избира друго k и се опитва отново.

Стъпка 6: Изчислява се стойността на s = (z + r d) / k mod n.

Стъпка 7: Ако s = 0, тогава се избира друга стойност на k и се опитва отново.

Двойката (r, s) формира подписа на алгоритъма ECDSA. За да провери подписа, Боб се нуждае от публичния ключ на Алис, от хеш z и от подписа (r, s). За проверката на подписа, Боб следва посочената по-долу процедура

Стъпка 1: Изчислява се $u_1 = s^{-1} z \bmod n$.

Стъпка 2: Изчислява се $u_2 = s^{-1} r \bmod n$.

Стъпка 3: Изчислява се точката $P = u_1 G + u_2 H_A$.

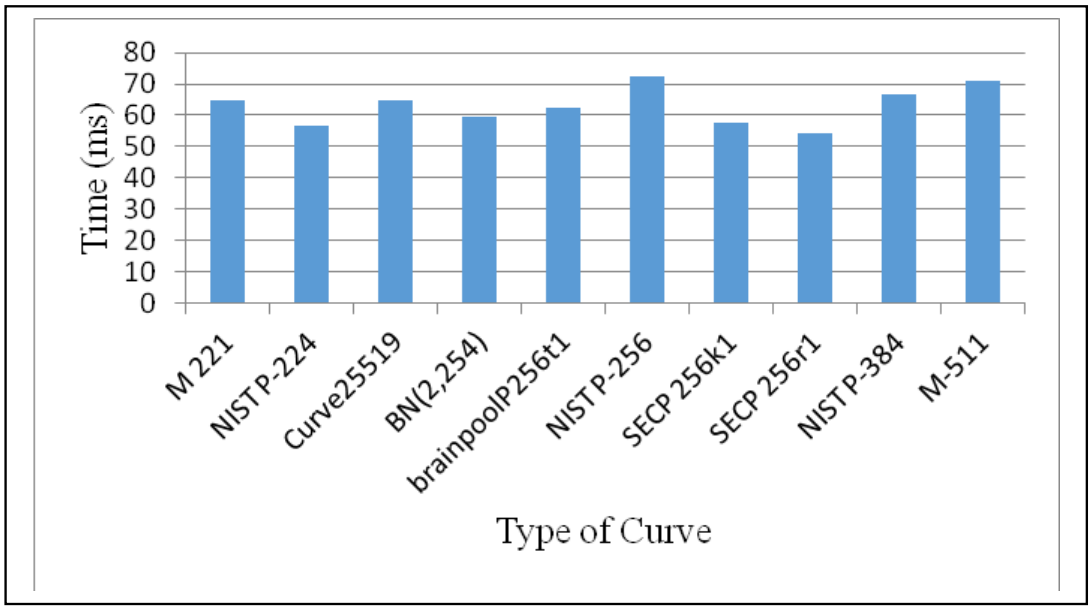
Подписът е валиден само ако r = xP mod n. (където xp е координата x на точката, изчислена както е показано в стъпка 3).

За анализ на различни елиптични криви се използва софтуерът SageMath [79]. Анализът се извършва, като се използва система, която има процесор Intel Core i3 с 4 GB RAM. Същата система и същият инструмент се използват при извършване на анализ на различни криви.

При ECDH алгоритъма се наблюдава времето за изчисление, необходимо за извършване на точково мултиплициране на крива по време на процеса на криптиране и времето за изчисление, необходимо за изчисляване на споделената тайна по време на процеса на декриптиране на ECDH алгоритъма за обмен на ключове. Таблица 2.5 показва изчислителното време, необходимо за всяка крива да изпълнява различни операции по време на ECDH алгоритъма за обмен на ключ. По подобен начин при ECDSA алгоритъма резултатите се разглеждат от гледна точка на изчислителното време, необходимо на всяка крива за изчисляване на подписа и времето, необходимо за проверка на подписа. Таблица 2.6 представя изчислителното време, необходимо на всяка избрана крива да извърши процеса на генериране и проверка на подписи, когато се използва за ECDSA.

Таблица 2.5. Време за изчисление за кривите при използване на ECDH алгоритъм

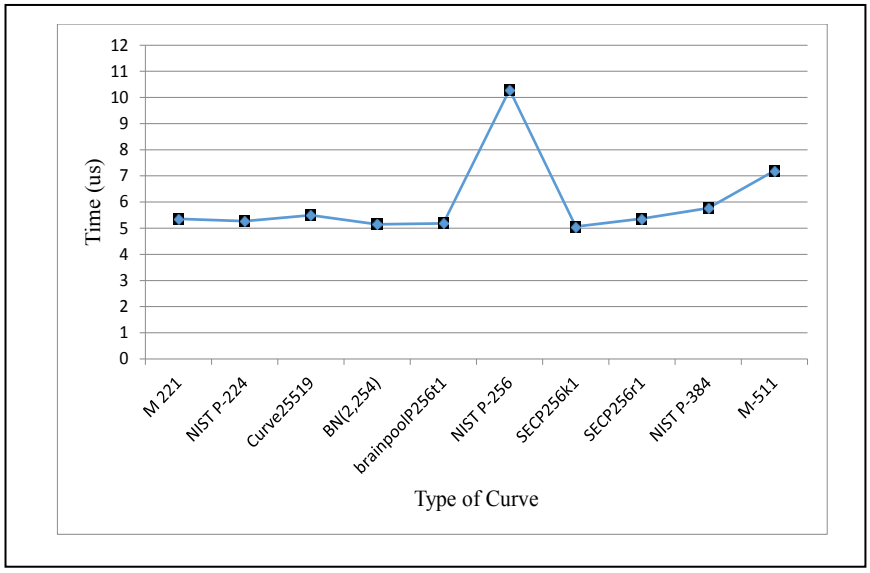
Type of curve	**Time taken for point addition** (ns)	**Time to calculate Alice's public key A(Kpb) = a*P** (ms)	**Time to calculate Bob's public key B(Kpb) = b*P** (ms)	**Time to calculate secret on Alice side a*B(Kpb)** (ms)	**Time to calculate secret on Bob side b*A(Kpb)** (ms)
M 221	136	17.9	15.1	15.6	16.2
NIST P-224	73.2	14.3	13.9	13.8	14.4
Curve25519	144	20.2	15.5	14.9	14.1
BN(2,254)	73.2	14.6	13.9	16.4	14.4
brainpoolP256t1	70.2	16.2	16.5	14.8	15.1
NIST P-256	68.7	14.8	20	17	20.4
SECP 256k1	67.1	13.9	15.4	14.3	13.9
SECP 256r1	78.2	13.7	13.3	13.6	13.7
NIST P-384	70.2	15.4	15.1	18.7	17.3
M-511	72.1	22.2	16.2	16.4	16.1



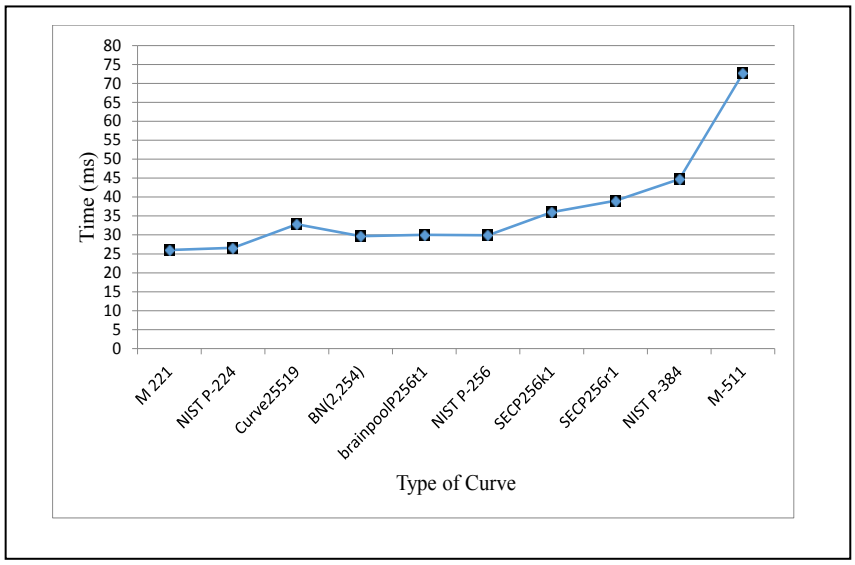
Фигура 2.5. Време на изчисление за всяка крива при ECDH алгоритъма

Таблица 2.7. Време за изчисление за кривите, когато се използват за ECDSA алгоритъма

Type of curve	**Time taken for Signature Generation (r, s)**		**Time taken for Signature Verification** (ms)
	Time to compute (r) (µs)	**Time to compute (s)** (µs)	
M 221	1.98	3.38	26
NIST P-224	1.73	3.54	26.6
Curve25519	2.06	3.44	32.8
BN(2,254)	1.68	3.47	29.7
brainpoolP256t1	1.78	3.40	30
NIST P-256	3.37	6.66	29.9
SECP256k1	1.73	3.33	36
NIST P-384	1.68	4.09	44.7
M-511	1.91	5.29	72.7



Фигура 2.6. Време за изчисление за всяка крива при генериране на подпис при ECDSA алгоритъма



Фигура 2.7. Време за изчисление за всяка крива при верификация на подпис при ECDSA алгоритъма

2.3 Заключение

Поради големия размер на ключовете RSA не е подходящ за среди, където работната мощност, съхранението, честотната лента или консумацията на енергия са ограничени. Тази глава предлага общ модел за сигурност на бизнеса с електронна търговия, използвайки криптографията на елиптичните криви, който е подходящ за системи с ограничен ресурс и който осигурява същото ниво на сигурност, подобно на RSA, но с по-малък размер на ключовете. В предложената система за електронна търговия ECC се

използва за криптиране на платежната информация заедно с информацията за поръчката на клиента. От анализа на различни криви е ясно, че с увеличаването на размера на полето на кривата, необходимото време за изчисление също се увеличава. В зависимост от изискването за сигурност на приложението и необходимото изчислително време трябва да бъде избрана подходящата елиптична крива. Таблица 2.5 и Таблица 2.6 показват времето за изчисление, което е необходимо за всяка крива за различни операции по време на ECDH и ECDSA алгоритмите. В приложения за електронна търговия, които използват смарт карти, безжични устройства и други подобни и където има по-малко място за съхранение и е необходима бърза обработка, може да се използва кривата SECP256r1 за реализация на ECDH алгоритъма и кривата M-221 за алгоритъма ECDSA.

2.4 Приноси към Глава 2

Тази глава има два основни приноса, свързани с подобряването на сигурността на електронната търговия, използвайки ECC.

- Изискването за сигурност на електронната търговия е анализирано и съответно се предлага нов модел за сигурност за електронна търговия, използващ ECC, който има по-добра изчислителна скорост, изисква по-малко памет и има по-малък размер на ключа в сравнение със съществуващия модел за сигурност, който използва алгоритъма RSA. В предложения модел ECC криптирането и декриптирането се използва за защита на информацията за поръчката на клиента и на информацията за плащането.

- Извършен е анализ на различни съществуващи елиптични криви, за да се установи коя крива е подходяща за приложение за електронна търговия, което има ограничени ресурси. Анализът се осъществява чрез прилагането на общи ECC алгоритми като ECDH и ECDSA за различни стандартни елиптични криви. Резултатите от анализа са представени в табличен вид за двата алгоритъма.

ГЛАВА 3. Проектиране на нов протокол за автентикация на потребител

Методът, който се използва за комуникация между оторизирани отдалечени потребители по несигурна мрежа, обикновено е система за автентикация, която използва специфична парола. Много потребители на електронна търговия използват автентикация въз основа на смарт карти по време на комуникация с отдалечените сървъри. Предложени са много техники за автентикация на отдалечени потребители, използващи смарт карта. Основната предимство от използването на смарт карта е наличието на памет и бързата обработка. Huang et al. [81] предлагат схема за автентикация на потребител със смарт карти, която използва концепцията за цифровото клеймо. За съжаление, Jung et al. [88] показват, че моделът на Huang не успява да отстрани офлайн атаката за разпознаване на парола и е трудно да се открие грешна

парола. В схемата на Huang се използва RSA криптосистемата за осигуряване на автентикация. В тази глава се предлага усъвършенстван и защитен протокол за автентикация на базата на смарт карти, използващ ECC. Така предложената схема преодолява всички възможни недостатъци на системата на Huang et al. и има по-голямо бързодействие в сравнение с другите налични методи.

3.1 Усъвършенстван протокол за автентикация на потребител със смарт карта, базиран на криптографията на елиптичните криви

Предложеният протокол за автентикация използва еднопосочна хеш функция вместо сложна симетрична криптосистема. Освен това RSA криптосистемата се заменя с ECC. Различните означения, използвани в предложените протоколи, са дадени в таблица 3.1. Предложеният протокол има четири фази, както е обяснено по-долу.

Таблица 3.1. Различни означения, използвани в предложения протокол

Notations	**Meaning**
U_A	The User
S	The server
k	The security parameter
q	A large prime number
F_q	A field of prime order q
E_q (a,b)	A set of elliptic curve points of order n, where a; b ϵ F_q
Q	A base point of order n over E_q (a,b)
$d_i : U_i$	The private/public key pair of the entity i, where i = A,S where $d_i \epsilon Z_q$ and $U_i = d_i * Q$
H ( )	One-way cryptographic hash function (e.g., MD5)
‖	The message concatenation operator
E (·)	The elliptic curve scalar point multiplication
A	The Adversary

A. Фаза на инициализация на системата

Това е първата фаза на предложения протокол, където системата се инициализира чрез избиране на различни параметри, както е обяснено по-долу.

Стъпка 1: В тази стъпка се избира крайно поле F_q за $q > 2^{160}$.

Стъпка 2: След избора на крайно поле е избрана елиптичната крива E_q (a,b) : y^2 mod q = x^3+ax+b mod q с ред n за F_q.

Стъпка 3: Избера се точка Q от ред n за E_q (a,b).

Стъпка 4: Елиптична крива E_q (a,b) и Q се представят в мрежата.

Стъпка 5: Потребител U_A и сървър S изберат техните частни и публични ключове като (d_A:U_A) и (d_S :Us)

където U_A= d_A*Q и U_S =d_S*.Q

B. Фаза на регистрация

По време на фазата на регистрация потребителят се регистрира на сървъра, като прилага следната процедура. Фазата на регистрация е изобразена на фигура 3.4.

Стъпка 1: Потребител U_A изпраща идентификатор ID_A и парола PW_A на сървъра S.

Стъпка 2: След това сървър S изчислява H_A = H ($PW_A \| d_S$) и R_A= H_A* Q.

Стъпка 3: Сървърът съхранява { ID_A,R_A,H(.),E_q,Q} на смарт картата .

C. Входна фаза

В тази фаза потребителя на картата изпълнява следната процедура, за да влезе в отдалечения сървър.

Стъпка 1: Потребител U_A избира текущото време като T_A и въвежда идентификационните си ID_A и парола PW_A.

Стъпка 2: Потребител U_A изчислява K_A=d_A*U_S.

Стъпка 3: След това потребител U_A изчислява C_A = H ($T_A \| ID_A \| K_A \| R_A$).

Стъпка 4: След това потребителят изпраща съобщение за заявка за вход към сървъра като M={ ID_A, C_A, T_A, R_A}.

D. Фаза на автентикация

След като съобщението за заявка за вход е получено от потребителя, сървърът S изпълнява следната процедура за автентикация на потребителя.

Стъпка 1: Сървърът S избира текущото време като T_S и проверява условието, че (T_S - T_A) ≤ ΔT, където ΔT е очакваното времезакъснение

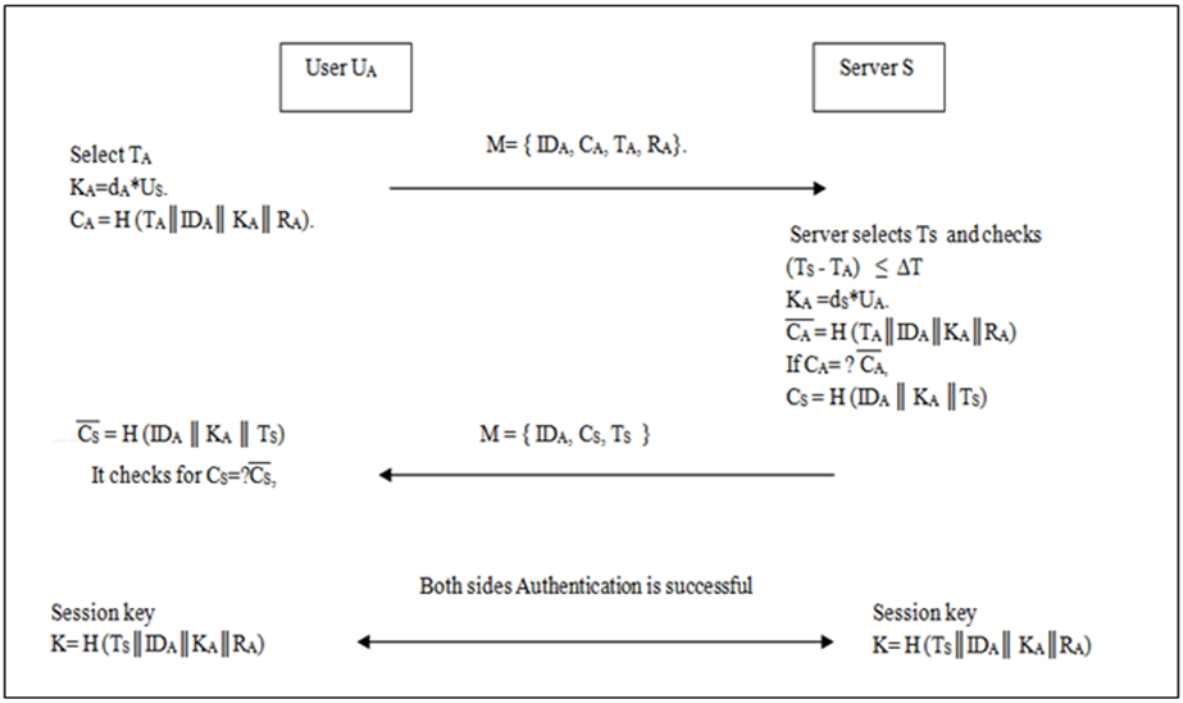
Стъпка 2: Сървър S изчислява стойността на K_A =d_S*U_A.

Стъпка 3: След това сървър S изчислява $\overline{C_A}$ = H ($T_A \| ID_A \| K_A \| R_A$) и проверява $\overline{C_A}$= ? C_A. Ако условието е удовлетворено, сървърът изпраща съобщението за автентикация на потребителя, в противен случай отхвърля искането за вход.

Стъпка 4: След това сървър S изчислява C_S = H ($ID_A \| K_A \| T_S$) и изпраща съобщение M ={ ID_A, C_S, T_S }на потребител U_A.

След получаване на съобщението за автентикация от сървъра, потребителят проверява автентичността на сървъра.

Стъпка 5: Потребител U_A изчислява $C_S = H(ID_A \| K_A \| T_S)$ и проверява $C_S =? C_S$. Ако условието е удовлетворено, сървърът се удостоверява и се създава ключът за сесията. Ключът за сесията се изчислява като $K = H(T_S \| ID_A \| K_A \| R_A)$.



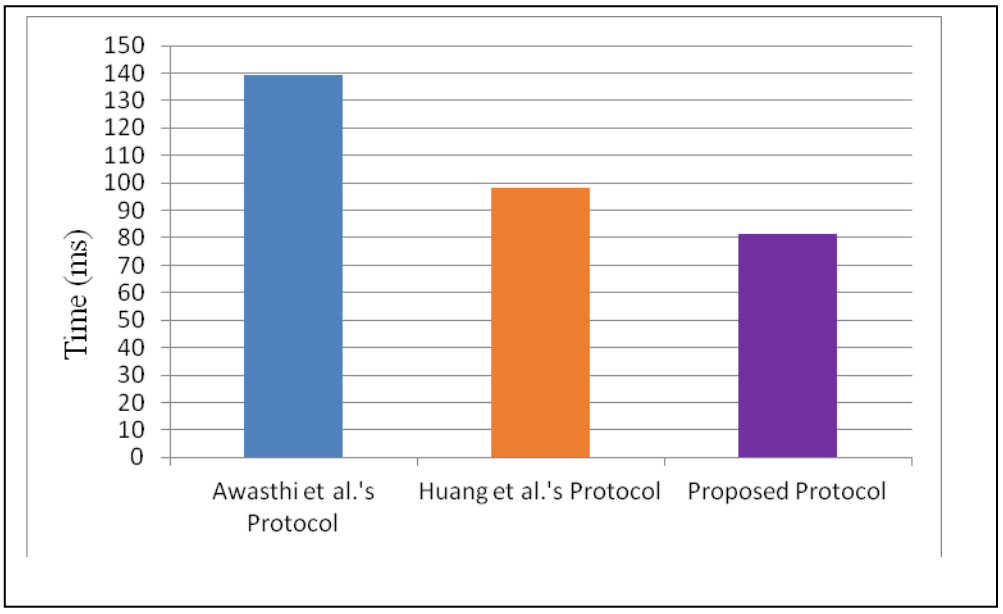
Фигура 3.5. Входна фаза и фаза на автентикация на предложения протокол

За да се определи ефективността на предложената схема, се използват различни параметри за анализиране на изчислителната сложност на протокола. Параметърът T_E означава времето, необходимо за едно модулно експоненциране, T_M означава времето, необходимо за едно модулно изчисление на умножение, T_H означава времето за изпълнение на еднопосочната хеш функция и T_{PM} означава времето за изпълнение на умножението на елиптичната крива. Таблица 3.2. показва резултата от сравнението на времето за изчисление, необходимо за различните схеми.

В предложения протокол потребителят се нуждае от двуточково умножение (T_{PM}) и три изчисления на хеш функцията (T_H), за да получи своята автентикация, а от друга страна, сървърът се нуждае от тройно умножение (T_{PM}) и четири изчисления на хеш функцията (T_H) за неговото удостоверяване. Времето, необходимо за модулното умножение и модулно експониране, е по-голямо от времето, необходимо за точковото умножение на елиптичната крива. Следователно, предложеният метод за автентикация е по-ефективен от протокола на Huang et al.(фиг. 3.8).

Таблица 3.2. Сравнение на изчислителната сложност на предложената схема с други схеми

Schemes	Computations for user to achieve authentication	Computations for server to achieve authentication
Awasthi et al.'s	$3T_E + 3T_M + 2T_H$	$3T_E + 1T_M + 3T_H$
Huang et al.'s	$2T_E + 2T_H$	$3T_E + 2T_H$
Proposed Scheme	$2T_{PM} + 3T_H$	$3T_{PM} + 4_{TH}$



Фигура 3.8. Общо време за завършване на процеса на автентикация при различни протоколи

3.2 Заключение

В тази глава се предлага защитен и ефикасен протокол за автентикация на потребител, който използва смарт карта, прилагайки криптографията на елиптичните криви. Предложеният протокол е защитен срещу различните онлайн атаки, като атака срещу представяне под чужда самоличност, повторна атака, атака за модифициране и атака „човек в средата". ECC изисква по-малък размер на ключовете и осигурява високо ниво на сигурност и бързодействие, така че използването на ECC със смарт карта предлага безопасна и по-бърза автентикация на отдалечен потребител. В таблица 3.2 са дадени данни, показващи ефективността на предложения протокол в сравнение с други протоколи за автентикация.

3.3 Приноси към Глава 3

Тази глава има един основен принос, свързан с проектирането на протоколи за автентикация на потребители на системи за електронна търговия.

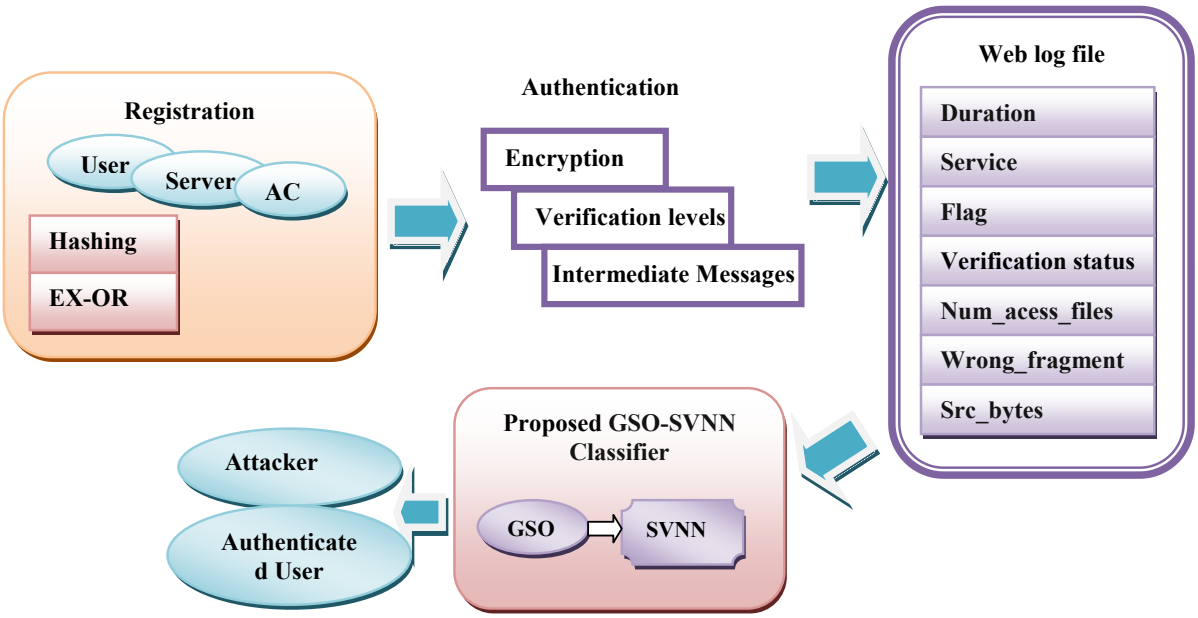
- Предложен е усъвършенстван и ефективен протокол за автентикация на потребители за системи за електронна търговия, използващ ECC. Разработеният протокол може да бъде използван за автентикация на легитимния потребител, когато той има достъп до отдалечения сървър със смарт карта. Тъй като в предложения протокол се използва ECC, той добавя по-малко изчислителна тежест към системата и е защитен срещу различни видове онлайн атаки. Изготвена е сравнителна таблица за изчислителното време, което се изисква от предложената схема, в сравнение със сходни съществуващи схеми. За да се докаже предимството на настоящия протокол, се извършва анализ на сигурността като се вземат предвид различните видове онлайн атаки.

ГЛАВА 4. Проектиране на нов класификатор за откриване на DoS атака по време на електронни търговски транзакции

4.1 ECC-базирана автентикация и оторизация на базата на оптимизирана векторна невронна мрежа за откриване на DoS атаки в електронните търговски транзакции

Широкото споделяне на ресурси в платформата за облачни изчисления я прави привлекателен инструмент през последните години за много приложения. Тя позволява потребителите да използват ресурсите си ефективно чрез статистическо мултиплексиране, а динамичното мащабиране намалява разходите за ресурси [91]. Увеличаването на броя на приложенията за електронна търговия, използващи изчислителни облаци, предизвика множество изследвания в областта на сигурността и поставя много ключови предизвикателства, включително проверка на целостта, автентикация, контрол на достъпа, предотвратяване на атаки и т.н. Един от основните рискове за сигурността в облачната платформа е атаката "DoS", която бе поставена на пето място през 2013 г. сред различни заплахи в облака от Алианса за сигурност в облака [93] [102]. Това е често срещана атака, причиняваща значителни загуби в облака. Въпреки че са разработени различни техники за облекчаване на DoS атаките, по-голямата част от съществуващите техники не се използват поради лошото им представяне.

Тази глава предлага техника за откриване на DoS атаки в транзакциите за електронна търговия, използваща автентикация на базата на ECC и нов GSO-SVNN класификатор. Тук облачният сървър и потребителят се регистрират първоначално и след това се удостоверяват с различни нива на проверка.



Фигура 4.2. Блокова диаграма на техниката за откриване на DoS атака, използвайки предложения GSO-SVNN класификатор

За верификация по време на автентикация се разменят няколко съобщения между потребителя, сървъра и Центъра за оторизация (AC) въз основа на хеширане и ECC криптиране. След като бъдат удостоверени, характеристиките като продължителност, услуга, флаг, състояние на потвърждение, num_access_files, wrong_fragment, src_bytes се извличат въз основа на поведението на потребителя от уеб дневника. С функциите, извлечени като вход, предложеният GSO-SVNN, който е разработен чрез интегриране на алгоритъма GSO в класификатора на SVNN, упълномощава потребителя. По този начин предложеният GSO-SVNN класификатор извършва детекция на DoS атака, като генерира два класа, а именно автентичен потребител и нападател. Процедурата за регистрация, предложена в тази техника, следва подхода на ECC. Преди автентикация на потребителя, е задължително потребителят и сървърът да бъдат регистрирани. Блоковата схема на предложената техника за откриване на DoS атака е представена на фиг. 4.2.

След успешната регистрация, предложената техника за откриване на DoS атаки изпълнява няколко нива на проверка чрез препращане на различни междинни съобщения, представени като S. Тук се вземат предвид четири съобщения и четири нива на проверка за автентикация.

Първоначално потребителят обединява I^U и P^U и криптира резултата, като използва съхранения частен ключ. Криптираният резултат отново се обединява с идентичността на потребителя, за да създаде съобщението S_1.

$$S_1 = \left(E_{K_+^U}\left(I^U \parallel P^U\right) \parallel I^U\right) \tag{4.5}$$

където $E_{K_+^U}$ представлява криптиране, използвайки ECC с K_+^U. Съобщението,

генерирано от потребителя, се проверява на сървъра, като се използва съхранената I^U и P^U, като

$$S_1^* = \left(E_{K^U}\left(I^U \parallel P_+^U\right) \parallel I_+^U\right) \tag{4.6}$$

където E_{K^U} представлява криптиране, използвайки ECC с K^U. Ако $S_1 = S_1^*$, то се счита за първо ниво на проверка, V_1. След това сървърът създава друго междинно съобщение, като шифрова идентичността на сървъра и паролата, както следва,

$$S_2 = \left(E_{K_+^S}\left(I^S \parallel P^S \parallel I^S\right)\right) \tag{4.7}$$

където $E_{K_+^S}$ представлява криптиране, използвайки ECC със съхранения частен ключ на сървъра K_+^S. Същото съобщение се потвърждава при AC, като се използва запаметеният ключ и идентичността на сървъра като,

$$S_2^* = E_{K^S}\left(I^S \parallel P_+^S\right) \parallel P_+^S \tag{4.8}$$

където E_{K^S} е ECC криптиране, използвайки K^S. Ако $S_2 = S_2^*$, то това е проверката на ниво 2, V_2. За третото ниво на потвърждение се създава съобщение в AC чрез EX-ORing на хешираният публичен ключ и на профила за данни на сървъра, както и

$$S_3 = D^S \oplus h\left(K^P\right) \tag{4.9}$$

където D^S и $h\left(K^P\right)$ посочват профила на данните на сървъра и хеширането на публичния ключ. Тогава съобщението се потвърждава на сървъра, използвайки съхраненото D^S,

$$S_3^* = D_+^S \oplus h\left(K^P\right) \tag{4.10}$$

където D_+^S е запаметеният профил за данни на сървъра. По този начин проверката на ниво 3, V_3, е пълна, ако $S_3 = S_3^*$. Четвъртото съобщение се генерира на сървъра, подобно на S_3, но с потребителския профил на данните, вместо D_+^S,

$$S_4 = D^U \oplus h\left(K^P\right) \tag{4.11}$$

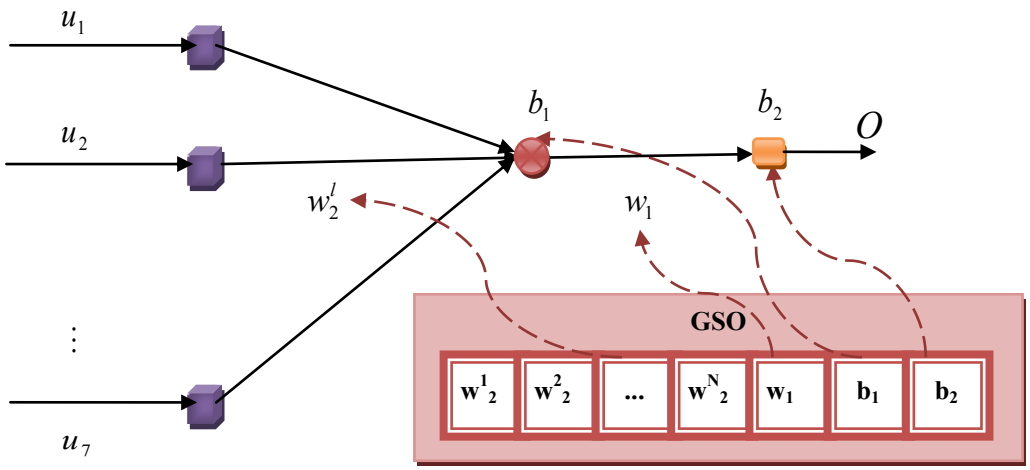
където D^U е профилът на данните на потребителя. Потребителят, заедно със съобщението S_4, намира потребителския профил на потребителя като,

$$D_*^U = h\left(K^P\right) \oplus S_4 \tag{4.12}$$

Ако условието $D_*^U = D_+^U$ е удовлетворено, това е проверката на ниво 4, V_4. По този начин, от четирите нива на проверка, потребителят може да бъде удостоверен, когато условието за верификация е изпълнено. Ако не, потребителят е нападател.

SVNN [113] се състои от три слоя, а именно входен слой, скрит слой и изходен слой. Въз основа на информацията, получена по време на фазата на автентикация, SVNN

класифицира потребителя или като нарушител, или като автентичен потребител. Предложената GSO-SVNN се реализира чрез обучение на SVNN с GSO [114], а не с генетичен алгоритъм (GA), така че работата на класификатора да се подобри благодарение на способността на GSO да решава проблеми с мултимодални функции. Архитектурата на предложената GSO-SVNN е показана на Фиг.4.3, където w_1 и w_2 показват теглата между скритите и изходните слоеве и между входните и скритите слоеве, а b_1 и b_2 представляват отклоненията при скритите и изходните слоеве, съответно.



Фигура 4.3. Архитектура на предложената GSO-SVNN

Техниките, взети за сравнение на ефективността на предложената техника, са Neighbor Similarity Trust [109], QADE [95], ECC + SVM (приложен SVM вместо GSO-SVNN в предложената техника), BARTD [108], ECC + SVNN (приложен SVNN вместо GSO-SVNN в предложената техника). Тук сравнителният анализ на предложената ECC + GSO-SVNN и съществуващите техники се извършва чрез промяна на процентите на данните за обучение.

Предложеният метод се реализира в MATLAB, като се използва Windows 10 OS и Intel® i3 процесор с 64-битова операционна система и 4GB RAM. Анализът се извършва с помощта на 4 опитни постановки. Резултатите за моделите във всяка от тях са описани по-долу.

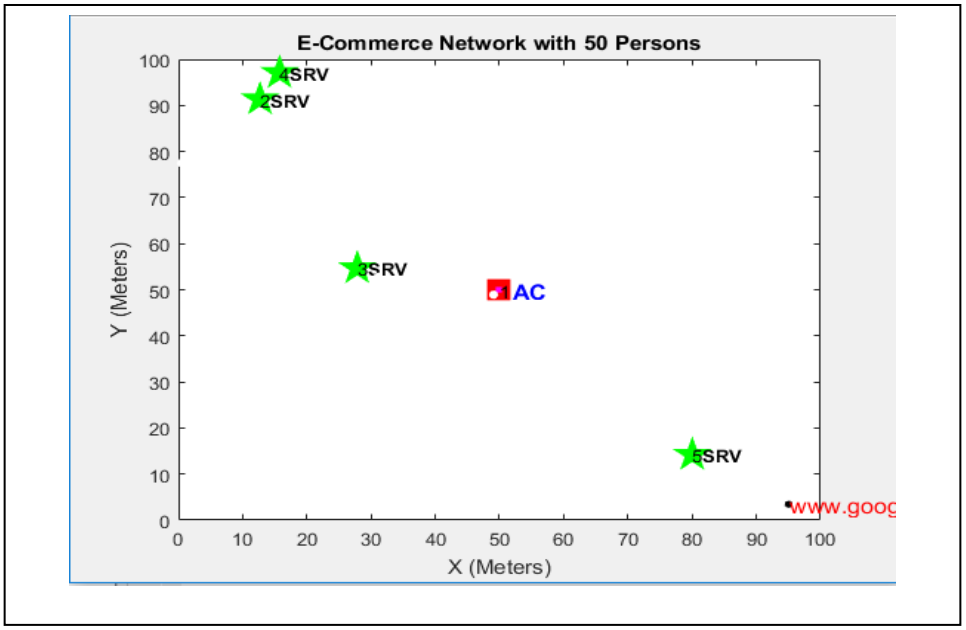
Опитна постановка 1: Симулация с 50 потребители и 5 нападатели.

Опитна постановка 2: Симулация с 75 потребители и 5 нападатели.

Опитна постановка 3: Симулация с 100 потребители и 10 нападатели.

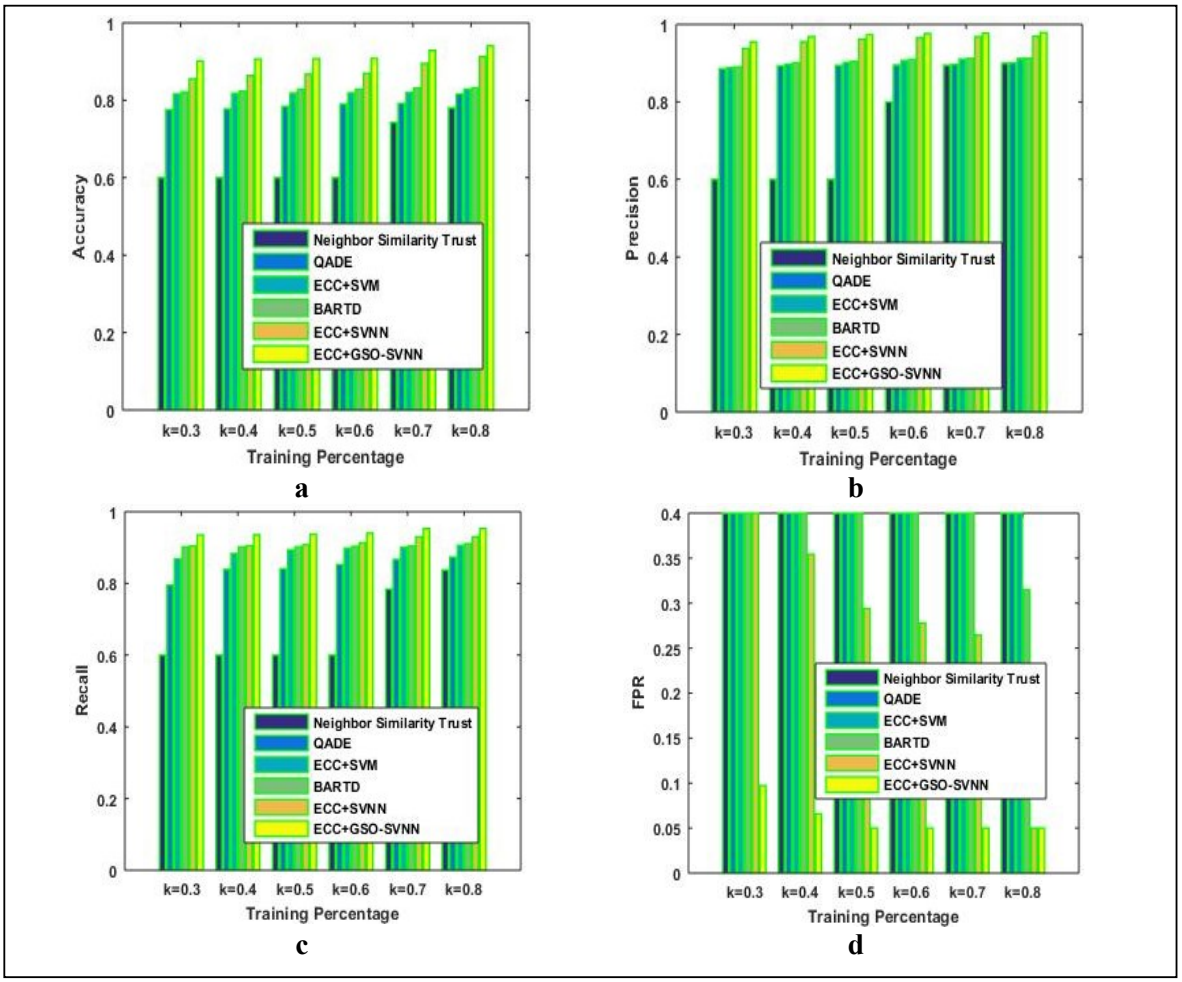
Опитна постановка 4: Симулация с 150 потребители и 15 нападатели.

При първата опитна постановка се разглежда модел с 50 потребители и 5 нападатели и се определят параметрите точност, прецизност, чувствителност и FPR. Fig.4.4. показва опитна постановка, при която 50 потребители участват в мрежа за електронна търговия. Тази мрежа има 4 легитимни сървъра, 1 център за автентикация и 5 нападателя.



Фигура 4.4. Опитна постановка, показваща мрежа за електронна търговия с 50 потребителя

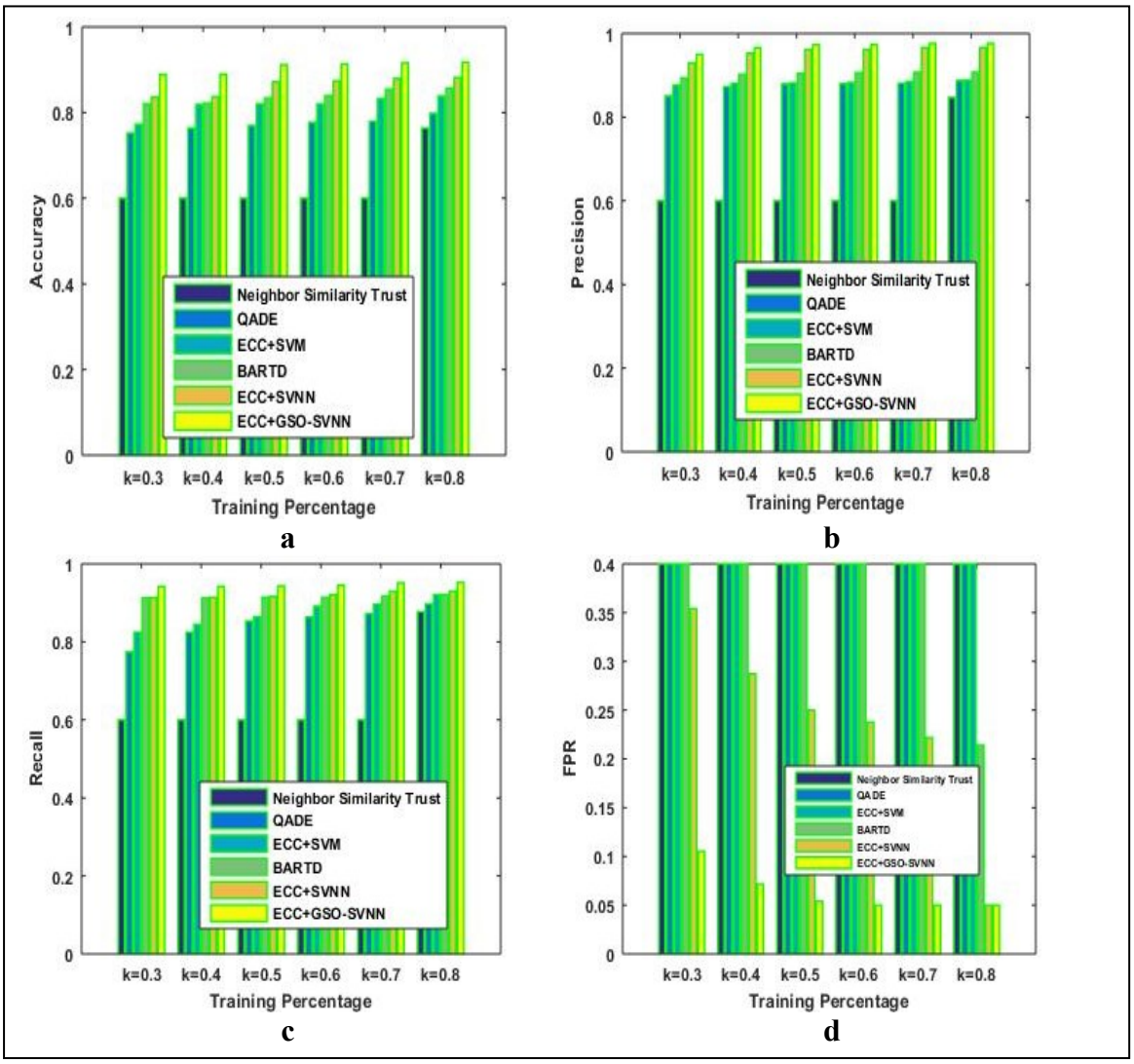
Фиг.4.5a илюстрира показателя за точност при променлив набор от данни за обучение, обозначени с k. При 80% данни за обучение съответната точност, измерена за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN, ECC + GSO-SVNN е 0.78, 0.816, 0.828, 0.832, 0.912 и 0.940, а 70% точността, измерена за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN, ECC + GSO-SVNN е съответно 0.742, 0.791, 0.8195, 0.831, 0.895 и 0.928. Следователно, предложеният метод прогнозира резултата с най-висока точност. Фиг.4.5b показва стойностите на параметъра за прецизност въз основа на данните за обучение, вариращи от 0.3 до 0.8. Когато данните са 80%, прецизността, измерена за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN и предложената ECC + GSO-SVNN е 0.899, 0.899, 0.911, 0.912, 0.969 и 0.978. Фиг.4.5c показва стойността на чувствителността, изчислена за Neighbor Similarity Trust, QADE, ECC + SVM, BAR TD, ECC + SVNN и предложената ECC + GSO-SVNN. За 80%, измерените стойности за чувствителността са съответно 0.837, 0.873, 0.906, 0.910, 0.93 и 0.952. Фиг.4.5d показва FPR анализ за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN и предложената ECC + GSO-SVNN. FPR за Neighbor Similarity Trust, QADE, ECC + SVM, BAR TD, ECC + SVNN и предложената ECC + GSO-SVNN е 0,4, 0,4, 0,4, 0,315, 0,05 и 0,05, съответно за k = 0.8. Изводът е, че предложеният метод показва по-добри резултати в сравнение с съществуващите методи.



Фигура 4.5. Резултати за опитна постановка 1 a) точност b) прецизност c) чувствителност d) FPR

Във втората опитна постановка се вземат предвид 75 потребители и 5 нападатели и се изследва точност, прецизност, чувствителност и FPR, а в третата опитна постановка 100 потребители участват с 6 удостоверени сървъра и един център за автентикация.

Четвъртата опитна постановка се състои от 150 потребители и 15 нападатели, участващи в мрежа за електронна търговия. Fig.4.11a илюстрира показателя за точност при променлив набор от данни за обучение, обозначени с k. За 80% данни, съответната точност, измерена за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN и предложената ECC + GSO-SVNN е 0.764, 0.798, 0.8384, 0.857, 0.882 и 0.917. Фигура 4.11b показва стойностите на прецизността въз основа на данните за обучение, вариращи от 0.3 до 0.8. Fig.4.11c представя чувствителността, изчислена за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN и предложената ECC + GSO-SVNN, а Fig.4.11d показва FPR анализ за Neighbor Similarity Trust, QADE, ECC + SVM, BARTD, ECC + SVNN и предложената ECC + GSO-SVNN.



Фигура 4.11. Резултати за опитна постановка 4 a) точност b) прецизност c) чувствителност d) FPR

Таблица 4.2. Сравнение на резултатите

Methods	**Accuracy**	**Precision**	**Recall**	**FPR**
Neighbor Similarity Trust	0.784	0.899	0.877	0.4
QADE	0.843	0.928	0.910	0.4
ECC+SVM	0.866	0.933	0.920	0.4
BARTD	0.873	0.934	0.940	0.4
ECC+SVNN	0.929	0.975	0.947	0.287
Proposed ECC+GSO-SVNN	**0.951**	**0.982**	**0.962**	**0.05**

Таблица 4.2. представя сравнителен анализ на съществуващите методи и предложения метод. От наблюдението е ясно, че предложеният метод превъзхожда съществуващите по всички показатели.

4.2 Заключение

Направен е литературен анализ на различни модели за сигурност, заедно с техните ограничения. Въпреки че са разработени различни техники за облекчаване на DoS атаките, по-голямата част от съществуващите техники не се използват поради лошото им изпълнение. Има много предизвикателства при проектирането на модели за откриване на DoS атаки при транзакции за електронна търговия, тъй те не могат да изпълнят всички изисквания за сигурна среда за онлайн бизнес. Съобразено с това в настоящата глава е разработена нова техника за откриване на DoS атаки в транзакциите за електронна търговия, използвайки предложения GSO-SVNN класификатор. Предложеният класификатор е проектиран чрез модифициране на SVNN, като се използва алгоритъм GSO, така че теглата да се избират оптимално. Първоначално потребителят и сървърът са регистрирани в облака за автентикация, който е проектиран с помощта на ECC криптиране и хеширане с четири различни нива на проверка и съобщения. След това се анализира поведението на потребителя, като продължителност, услуга, флаг, състояние на потвърждение, num_access_files, wrong_fragment, src_bytes, за да се даде разрешение. Предложената GSO-SVNN класифицира потребителя като автентичен потребител или атакуващ въз основа на извлечената информация. Експериментите са за четири показателя: точност, прецизност, чувствителност и FPR, с цел да се оцени ефективността на предложената техника. Резултатите показват, че предложената техника за откриване на DoS атаки е ефективна при откриване на атаки в електронните търговски сделки с 95.1% точност.

4.3 Приноси към Глава 4

Тази глава има два основни приноса, свързани с проектирането на механизъм за откриване на DoS атаки в системи за електронна търговия.

- Разработена е процедурата за регистрация и удостоверяване на автентичността между потребителя и сървъра, която има четири различни нива на проверка, като се използва ECC и хешираща функция с идентичност, парола, личен ключ и профил на данните на участниците. Тази процедура е полезна за регистриране и автентикация на потребителя и сървъра с AC в облака.

- Разработен е мощен механизъм за откриване на DoS атаки, използващ GSO-SVNN, за защита на транзакциите за електронна търговия. Предложената техника е сравнена със сходни съществуващи модели. Резултатът показва, че тя е по-ефективна в сравнение с наличните техники за откриване на DoS атаки.

III. ЗАКЛЮЧЕНИЕ И ОСНОВНИ ПРИНОСИ

Темата на този дисертационен труд е свързана със сигурните и ефективни техники базирани на криптографията с елиптични криви за защита на транзакциите при електронна търговия, като целта е да се разработи и развие сигурна, ефективна, проста и надеждна техника за автентикация, използваща елиптична крива, която да се използва в приложения за електронна търговия с ограничени ресурсите, които имат изискване за висока степен на сигурност, и за проектиране на сигурна и надеждна техника за оторизиране, за да се защитят транзакциите от електронна търговия от DoS атаките. За да се изпълни гореспоменатата цел, са разработени различни протоколи и техники, които осигуряват сигурна и ефективна среда за системата за електронна търговия, като осигуряват услугите за автентикация, оторизация и интегритет по време на сделките за електронна търговия.

Основните приноси на дисертацията са изброени по-долу.

1. Създаден е нов модел за защита на системата за електронна търговия, използващ ECC, който има по-голямо бързодействие, изисква по-малко памет и има по-малък размер на ключа в сравнение със съществуващите модели за сигурност, които използват алгоритъма RSA. В предложения модел ECC криптирането и декриптирането се използват за защита на информацията за поръчката на клиента както и информацията за плащането.

2. Извършен е анализ на различни налични елиптични криви, за да се установи коя крива е подходяща за приложение за електронна търговия с ограничени ресурси. Анализът се осъществява чрез прилагането на общи ECC алгоритми като ECDH и ECDSA за различни стандартни елиптични криви.

3. Предложен е усъвършенстван и ефективен потребителски протокол за автентикация, използващ ECC. Протоколът се използва за валидиране на легитимен потребител, когато потребителят има достъп до отдалечения сървър със смарт карта. Тъй като в предложения протокол се прилага ECC, той добавя по-малко изчислителен товар към системата и е защитен срещу различни видове онлайн атаки.

4. Разработена е процедура за регистрация и автентикация между потребителя и сървъра, при която са развити четири различни нива на проверка, като се използва ECC и хешираща функция с идентичност, парола, личен ключ и профил на данните на участниците. Тази процедура е полезна за регистриране и автентикация на потребителя и сървъра с AC в облака.

5. Разработен е мощен механизъм за откриване на DoS атаки, който използва GSO-SVNN за защита на електронните търговски транзакции. Методът е

симулиран и резултатите се сравняват със сходни съществуващи модели. Резултатът показва, че предложената техника е по-ефективна в сравнение с наличните техники за откриване на DoS атаки.

IV. ИЗПОЛЗВАНИ СЪКРАЩЕНИЯ

AC- Authorization Center

CRAM- Cyber-Risk Assessment and Mitigation

DoS- Denial of Service

DDoS-Distributed Denial of Service

E-commerce- Electronic Commerce

ECC- Elliptic Curve Cryptography

EDI- Electronic Data Interchange

EFT-Electronic Funds Transfer

ECDLP- Elliptic Curve Discrete Logarithm Problem

ECDSA- Elliptic Curve Digital Signature Algorithm

ECDH- Elliptic Curve Diffie-Hellman

FPR- False Positive Rate

GA- Genetic Algorithm

GSO- Glowworm Swarm optimization

GSO-SVNN- Glowworm Swarm optimization-Support Vector Neural Network

RSA- Rivest, Shamir, and Adelman

SVNN- Support Vector Neural Network

V. СПИСЪК НА ПУБЛИКАЦИИТЕ КЪМ ДИСЕРТАЦИЯТА

[A1] Javed Shaikh, Sachin D.Babar and Georgi Iliev, "E-commerce Development with Respect to its Security Issues and Solutions: A Literature Review," in Proc. of 52nd International Scientific Conference on Information, Communication and Energy Systems and Technologies, Nis Serbia, pp. 165-168, 28-30 Jun.2017.

[A2] Javed R. Shaikh,Vandana M. Rohokale and Georgi Iliev, "State of the Art Protection Techniques against Denial of Service Attacks In E-commerce Network," in Proc. of Global Wireless Summit (GWS), Aarhus, Denmark, 27-30 Nov.2016.

[A3] Javed R. Shaikh, Ravinder Kumar, Maria Nenova, Georgi Iliev and Hitesh Singh, "Enhancing E-commerce Security using Elliptic Curve Cryptography," International Journal of Current advanced research. Vol. 6, Issue 8, pp. 5338-5342, Aug. 2017.

[A4] Javed R. Shaikh, Maria Nenova and Georgi Iliev, "Analysis of Standard Elliptic Curves for the Implementation of Elliptic Curve Cryptography in Resource Constraint E-commerce Applications," in Proc. of IEEE International Conference on Microwaves, Communications, Antennas and Electronic Systems. pp. 1-4, Tel Aviv, Israel, 13-15 Nov.2017.

[A5] Javed R. Shaikh and Georgi Iliev, "Advanced Smart Card based User Authentication Protocol using Elliptic Curve Cryptography," in Proc. of 5th International conference

for Sustainable Global Development, IEEE INDIACom, Delhi, pp. 2474-2478,14-16 Mar.2018.

[A6] Javed R. Shaikh, "ECC Based Authentication and Optimized Support Vector Neural Network based Authorization for Detection of DoS Attack in the E-commerce Transactions," International Journal of Current Engineering and Scientific Research , Vol. 5, Issue 2, pp. 47-54, Feb. 2018.

[A7] Javed R. Shaikh, Ravinder Beniwal and Georgi Iliev "Cryptography and Optimization Driven Support Vector Neural Network to Mitigate DoS Attacks in E-commerce" in Proc. of Springer International Conference on Manufacturing, Advanced Computing, Renewable Energy and Communication (MARC), Delhi, India,19-20 July 2018.

VI. ЛИТЕРАТУРНИ ИЗТОЧНИЦИ

[1] K. Ahmed and M. S. Alam, "E-commerce Security Through Elliptic Curve Cryptography," in Proc. International conference on information security & Privacy, Nagpur, India, pp. 867-873, 11-12 Dec. 2015.

[3] A. Haidari and K. Paktiani, "A study about trust and security within E-commerce," University of Gothenburg , Gothenburg Sweden, Mar. 2011.

[7] S. T. Lai, F. Y. Leu and W. C. Chu, "A Multi-Layer Secure Prevention Scheme for Improving E-commerce Security," in Proc. Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 505-510, 2014.

[11] Y. Zhang, X. Deng, D. Wei and Y. Deng, " Assessment of E-Commerce security using AHP and evidential reasoning," Journal of Expert Systems with Applications, Elsevier, Vol. 39, pp. 3611-3623, 2012.

[26] S. Chatterjee, " Security and Privacy Issues in E-Commerce: A Proposed Guidelines to mitigate the Risk," IEEE, pp. 393-396, 2015 .

[27] X. Wang, Y. Jio and L. Guo, "Study on the function of computer technology in the electronic commerce environment security and risk assessment," in Proc. IEEE International Conference on Intellegant Transportation,Big Data and Smart City, pp. 784-786, 2016.

[30] J. Chen and X. Xie , "The Security of Shopping Online," in Proc. International Conference on Electronic & Mechanical Engineering and Information Technology, pp. 4693-4696, 2011.

[31] F. Zhu and G. Li , "Study on Security of Electronic Commerce Information System," IEEE, pp. 1546-1549, 2011.

[34] F. Y. Leu , C. H. Lin and A. Castiglione , "Special issue on cloud, wireless and e-commerce security," Journal of Ambient Intelligence and Humanized Computing, Springer , pp. 207–208, 2013.

[47] S. Yasin, K. Haseeb and R. J. Qureshi, "Cryptography Based E-commerce Security:A Review," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, Mar. 2012.

[53] M. Mindi, "Cyber Security Tip ST04-015 - Understanding Denial-of-Service Attacks," Archived from the original on 2013-11-04. Retrieved December 11, 2013.

[57] Corero Network Security Releases, “Second Annual DDoS Impact Study,” Retrived from http:// www.coreo.com, Mar. 2016.

[61] I. K. Salah, A. Darwish and S. Oqeili, “Mathematical attacks on RSA cryptosystem,” Journal of Computer Science, Vol. 2, pp. 665-671, Aug. 2006.

[62] C. S. Benjamin and U. Alpay , “Advantage of using Elliptic curve cryptography in SSL/TLS,” Department of Computer Science University of California Santa Barbara, cs 290G fall term, 2015.

[67] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shanrz, “Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs,” CHES 2004,LNCS 3156, pp. 119-132, 2004.

[79] www.sagemath.org

[81] H. F. Huang, H. W. Chang and P. K. Yu, “Enhancement of timestamp-based user authentication scheme with smart card,” International Journal of Network Security, Vol. 16, no. 6, pp. 463-467, Nov. 2014.

[88] J. Jung, Y. Choi, D. Lee, J. Kim and D. Won, “Security Weaknesses of a Timestamp-Based User Authentication Scheme with Smart Card,” International Journal of Information and Education Technology, Vol. 5, no. 7, Jul. 2015.

[[93] J. Cao, B. Yu, F. Dong, X. Zhu and S. Xu, "Entropy‐based denial‐of‐service attack detection in cloud data center," Concurrency and Computation: Practice and Experience, Vol. 27, no. 18, pp. 5623-5639, 2015.

[102] TTW Group, "The notorious nine: Cloud computing top threats in 2013," Report, Cloud Security Alliance, 2013.

[113] O. Ludwig, U. Nunes and R. Araujo, "Eigen value decay: A new method for neural network regularization", Neurocomputing, Vol. 124, pp. 33–42, 2014.

[114] K. N. Kaipa and D. Ghose, "Glowworm Swarm Optimization: Algorithm Development," Glowworm Swarm Optimization, Springer International Publishing, pp. 21-56, 2017.

TECHNICAL UNIVERSITY OF SOFIA
FACULTY OF TELECOMMUNICATIONS
DEPARTMENT OF "COMMUNICATION NETWORKS"

Javed Rasheed Shaikh

Elliptic Curve Cryptography Based Secure and Efficient Techniques to Protect E-commerce Transactions

ABSTRACT of Ph.D THESIS

The title of this thesis is related to elliptic curve cryptography based secure and efficient techniques to protect E-commerce transactions, with the goal defined as to design and develop secure, efficient, lightweight and reliable authentication technique using elliptic curve cryptography that could be implemented in resource-constrained E-commerce applications having high-security requirement and to design of secure and trustworthy authorization technique to protect the E-commerce transactions from the denial of service attacks. To fulfill the above stated goal various protocols and techniques are developed which provides the secure and efficient environment to the E-commerce system by proving the authentication, authorization and integrity services during the E-commerce transactions.

The thesis consists of 4 chapters, 50 figures, 13 tables and 34 mathematical expressions. The number of references is 114 with 82 % from the last 10 years. The analysis, proposed methods and results are presented through 7 author publications, 2 of which are in international scientific journals and 5 are presented at international conferences. chapter 1 provides a survey of security issues and its available solutions in E-commerce along with the survey of impact of DoS and DDoS attack on E-commerce system; chapter 2 proposes novel security model for the E-commerce using elliptic curve cryptography and analysis of standard elliptic curve is performed to find out the suitable curve for ECC implentation in resource constrained E-commerce applications; chapter 3 gives the design of advanced new user authentication protocol using the smart card and chapter 4 proposes the authentication and authorization model using Glowworm Swarm optimization-Support Vector Neural Network (GSO-SVNN) to mitigate the DoS attack in E-commerce transactions.

The major contributions of the thesis are listed below. 1) The proposal for new security model for E-commerce system using ECC along with the the analysis of different available elliptic curves is performed to find out which curve is suitable for the resource-constrained E-commerce application. 2) The design and development of a advanced secure and efficient user authentication protocol using to validate the legitimate user when the user is accessing remote server with his/her smart card. 3) The development of procedure for the registration and the authentication between the user and server where four different levels of verification are designed using ECC and hashing function to register and authenticate the user and server with AC in the cloud environment. 4) Design and development of the robust DoS attack detection mechanism is developed using Glowworm Swarm Optimization based Support Vector Neural Network (GSO-SVNN) to protect the E-commerce transactions.